AntiVirenKitT 5

AntiVirenKitT 5

AntiVirenKitT 5

ZASTOSOWANIA

Wersja uruchamiana przez **AUTOEXEC.BAT**

Wersja **DOS**'owa

SZATA GRAFICZNA WINDOWS

TAJNIKI I SZTUCZKI

Włożenie dyskietki startowej do stacji

INFORMACJA O WIRUSACH

Katalog wirusów

Na początek krótkie wprowadzenie.

Zdecydowaliście się Państwo na ochronę, przed komputerowymi wirusami, poprzez zastosowanie programu **AntiVirenKit5**. Nabyty przez Państwa produkt, jest wynikiem siedmioletnich doświadczeń i wnikliwych badań, które doprowadziły do zastosowania najnowocześniejszej technik programistycznych. Produkt, który Państwo już posiadacie, jest dla każdego łatwy w obsłudze, ale równocześnie pewny i skuteczny w działaniu. Skuteczność i pewność, w połączeniu z prostą intuicyjną obsługą, to główne hasła, które przyświecały nam podczas programowania **AVK5**. Obecna wersja programu przedstawia, jeszcze nieosiągnięty do tej pory, bardzo wysoki poziom software.

Aby posiadana przez Państwa wersja **AVK5**, pozostała stale aktualna, zalecamy regularne uaktualnianie programu poprzez: SERWIS PRYWATNY lub SERWIS PROFESJONALNY.

AntiVirenKit5 chroni od wielu lat, cenne dane banków, urzędów, małych i dużych zakładów pracy, przed niepotrzebnymi niespodziankami oraz dużymi stratami finansowymi.

AntiVirenKit5 jest tak zaprogramowany, że rozpoznaje nie tylko znane wirusy, ale także, przy użyciu różnych technik, rozpoznaje nowe - jeszcze nieznane wirusy.

Zakup **AntiVirenKit5** jest dobrą inwestycją. Program ten będzie służył Państwu przez długie lata, zapobiegając i chroniąc, a w wypadku przedostania się wirusa do systemu; podejmie działanie w celu jego usunięcia. Przy rozwiązywaniu wynikłych stąd problemów, każdy zarejestrowany użytkownik programu, otrzyma bezpłatnie pomoc poprzez tzw. **Gorącą Linię** (Hotline).

Tak więc życzymy Państwu wiele przyjemności, w obsłudze **AntiVirenKit5**, oraz sukcesów we wspólnej działalności profilaktycznej; skierowanej przeciwko wirusom komputerowym.

LTP MediaSoftware-G DATA Software Sp. z o.o., listopad 1995.

LTP MediaSoftware - G DATA Software - serwis

W pierwszy rzędzie, to co najważniejsze:

Prosimy Państwa, o wypełnienie karty rejestracyjnej programu i jej niezwłoczne odesłanie !

Tylko w taki sposób, jest możliwe zapewnienie wsparcie, ze strony naszego serwisu i korzystania z:

- bezpłatnej tzw. **Gorącej Linii** (HotLine)
- PRYWATNEGO SERWISU
- wirusowego serwisu.

Przy wypełnianiu karty rejestracyjnej, w przypadku gdy oznaczymy pole: SERWIS PROFESJONALNY, to zapewnimy sobie stałą dostawę nowych wersji programu antywirusowego **AntiVirenKit5**.

Jeżeli jednak nie zdecydujecie się Państwo od razu, na ten krok, to jest zawsze możliwe skorzystanie w późniejszym terminie, z tej dogodnej formy stałej współpracy.

*Wersja naszego programu, która dotrze do Państwa, może mieć kilka tygodni, i nie jest w stanie zapewnić pełnej ochrony - przed najnowszymi wirusami !!! Dlatego też, każdy zarejestrowany użytkownik, otrzyma od nas **bezpłatnie**, po przesłaniu karty rejestracyjnej, dyskietkę z najnowszą wersją programu **AntiVirenKit5.** Dzięki temu nie musicie Państwo martwić się, czy zakupiona wersja jest najnowsza - my dostarczymy Państwu zawsze najnowszą wersję programu !!!*

Numer Rejestracyjny.

W pudełku, z programem znajduje się karta rejestracyjno - serwisowa. Proszę wypełnić ją (uważnie) i odesłać do nas. Tylko w ten (prosty) sposób, możemy Państwa zarejestrować oraz w razie potrzeby udzielić pomocy. Nasz serwis zawsze pyta i... sprawdza numer rejestracyjny użytkownika. Numer ten znajduje się także na ostatniej stronie oryginalnego podręcznika. Numer ten będzie także potrzebny Państwu, w przypadku późniejszej akcesji w SERWISIE PROFESJONALNYM.

Wymiana dyskietki z programem.

Każda oryginalna dyskietka z programem, która uległa zniszczeniu lub niewłaściwie funkcjonuje zostanie **bezpłatnie** wymieniona. W celu dokonania takiej wymiany należy; przesłać (do nas) uszkodzoną dyskietkę wraz z ofrankowaną kopertą zwrotną.

Tylko przesyłki spełniające powyższe warunki będą mogły być rozpatrywane.

Doradztwo w sprawie wirusów.

Jeżeli "odkryliście" Państwo nowego wirusa lub zaobserwowaliście, niewytłumaczalne zachowanie się sprzętu komputerowego (oprogramowania), to prosimy o przesłanej nam, jak najszybciej, dyskietki z kopią tego programu. Po przeanalizowaniu dyskietki, postaramy się jak najszybciej zaproponować Państwu odpowiednie rozwiązanie. Jeżeli ocena **AVK5**, zobliguje Państwa do wysłania nam podejrzanego programu, to proszę to uczynić niezwłocznie.

My, ze swojej strony, zobowiązujemy się do używania Państwa plików, z zachowaniem najwyższej dyskrecji i poufności dostarczonych zbiorów !!

Aktualizacja programu.

AVK5 jest stale unowocześniany i rozwijany. Biorąc pod uwagę, że ciągle pojawiają się nowe, nie rzadko "inteligentne" wirusy, to wersja programu, która ma kilka tygodni nie zapewnia dostatecznego bezpieczeństwa. Rocznie wydajemy od 8 do 10 uaktualnień programu (nowych wersji), co daje w przeliczeniu co 6-8 tygodni dyskietkę z... najnowszym stanem wiedzy o wirusach.

Dla Państwa własnego bezpieczeństwa, jest bardzo ważne, abyście Państwo posiadali zawsze najnowszą, a tym samy aktualną wersję **AntiVirenKit5**. W ten sposób zapewniacie Państwo sobie, rozpoznania i usuwanie, przez program, również najnowszych wirusów.

Do otrzymania uaktualnienia programu wiodą dwie drogi:

SERWIS PRYWATNY
SERWIS PROFESJONALNY

Serwis Prywatny

Ten serwis jest bezpłatny, dla każdego zarejestrowanego użytkownika. Po przesłaniu (na adres naszej firmy) **oryginalnej dyskietki programu AVK5** oraz **ofrankowanej zwrotnej koperty**, otrzymacie Państwo bezpłatnie, najnowszą wersję programu.

Prosimy nie przysyłać opakowań i książek obsługi programu !!!

Serwis Profesjonalny.

Ciągłe pamiętanie, o zakupie nowej wersji programu (UpGrade) jest nader kłopotliwe, a konsekwencje użytkowania starej sesji, mogą oznaczać dla Państwa i Państwa Firmy wielkie niebezpieczeństwo. Aby tego uniknąć, proponujemy Państwu: SERWIS PROFESJONALNY, który zapewnia otrzymanie zawsze nowej i aktualnej wersji naszego programu.

Z chwilą opracowania nowej wersji; natychmiast prześlemy ją Państwu, wraz z gazetką firmy G DATA "Viren News", w której to, znajdują się informacje o postępie badań firmy G DATA nad wirusami. Gazetka ta z przyczyn technicznych ukazuje się na razie w języku niemieckim. Planowane jest wkrótce wydawanie wersji polskiej.

Na SERWIS PROFESJONALNY można się zdecydować podczas wypełniania karty rejestracyjnej lub w późniejszym - nieokreślonym czasie. SERWIS PROFESJONALNY trwa jeden rok i jest co roku odnawiany, a o terminie jego odnowienia jesteście Państwo informowani.

Firma nasza zaleca wszystkim naszym klientom (posiadającym firmy) skorzystanie z tego serwisu. Inwestycja ta zwraca się nieomal natychmiast... po zawarciu umowy! Bezpieczeństwo Państwa danych jest największym majątkiem firmy. Tego samego zdania jest wiele firmy zachodnich, które korzystają z naszego serwisu od lat. Na życzenie udostępniamy listę referencyjną.

Jeżeli używacie Państwo komputera do pracy, jest to dla szczególnie ważne, ażeby programy oraz dane chronić przed inwazją wirusów, gdyż zgromadzone dane posiadają, jak już wspomniano, bezcenną wartość. Poza tym dla wielu firm, instytucji oraz profesjonalnych użytkowników komputerów, jest stratą czasu wysyłanie kopert oraz dyskietek, a i tak nie gwarantuje to posiadania najnowszej wersji programu. W tym wypadku SERWIS PROFESJONALNY odciąży Państwa, od powyższych problemów!

Niedotrzymanie zasad umowy serwisowej

Nasze bogate świadczenia serwisowe mogą być tylko wtedy zrealizowane, gdy ograniczymy do minimum jego koszty własne. Dlatego, gdy chcesz skorzystać z naszego serwisu, prosimy o zastosowanie się do jego zasad.

Wysyłka dyskietek

Podczas wysyłki dyskietki z nieznanym wirusem prosimy o przestrzeganie następujących zasad:

- każda wysłana dyskietka musi posiadać etykietkę z nazwą, adresem oraz numerem telefonu wysyłającego
- na etykietce dyskietki, prosimy wpisać wersję programu **AVK5**, która była użyta.

Generalnie prosimy, przy przesyłaniu wszelkich dyskietek do naszej firmy, o przestrzeganie następujących zasad:

- przesyłki polecone są z reguły niekonieczne
- dyskietki z pismem towarzyszącym (objawy działania) mogą być wysłane jako list zwykły
- prosimy używać, do wysyłanych dyskietek, specjalistycznych kopert, a w przypadku ich braku; dyskietkę należy obłożyć kartonem.

Pliki tekstowe (*.TXT).

Stałe rozwijanie i uaktualnianie programu **AVK5** powoduje, że część najnowszych informacji nie znajduje się w podręczniku, a jedynie w pliku tekstowym , które można odczytać pod dowolnym edytorem. Najprostszym sposobem jest wykorzystanie polecenia MSDOS'a **TYPE**, w postaci jn.

TYPE {stcja_dyskietek}:\ANTIVIR.TXT

lub wydrukować - używając

TYPE {stcja_dyskietek}:\ANTIVIR.TXT >PRN

W środowisku Windows możemy wykorzystać **Notatnik** ze standardowych **Akcesoriów** (w **Menedżerze programów**).

Prosimy pamiętać, że informacje zawarte w pliku tekstowym mają zawsze priorytet, w stosunku do tekstu podręcznika.

Szybkie Startowanie programu AVK5

Zanim po raz pierwszy uruchomisz program AVK5...

W żadnym wypadku nie wolno instalować programu **AVK5** lub jakiegokolwiek innego, gdy podczas analizy wstępnej zostały wykryte wirusy na twardym dysku lub w pamięci komputera, lub został wyświetlony komunikat o ich przypuszczalnym istnieniu!

Proszę Państwa! Nadszedł czas przekonania się, czy nasz program **AntiVirenKit5**, czasem nie...znalazł jakiś wirusów.

Najpierw przeprowadzamy tzw. "Szybką Analizę" wirusów na podstawie opisu "Szybkiego Otwierania":

Szybkie otwieranie programu AVK5

1. należy wyłączyć komputer
2. należy na nowo uruchomić komputer, z wolnej od wirusów dyskietki
3. należy uruchomić wersję DOS'ową programu **AVK5** wywołując **AVK.EXE**.

Po wykonaniu, powyższych operacji, można komputer na nowo włączyć i zainstalować aktualną wersję **AVK5** .

Prosimy powtórnie sprawdzić , czy **AVK5** nie znalazł wirusów lub czy wszystkie wcześniej rozpoznane, zostały usunięte!.

Wersja programu uruchamiana "BATCH'em" .

Przy tej wersji **AVK5** zrezygnowaliśmy z graficznej powierzchni obsługi programu, gdyż chodzi tutaj głównie o szybkie przeszukiwanie plików twardego dysku podczas startu komputera. Poza tym program daje się wygodnie obsługiwać z poziomu DOS'a, w celu szybkiego przeszukiwania i sprawdzania wspomnianego dysku twardego oraz dyskietek. Istnieje możliwość przeszukiwania całego dysku, wybranej części drzewa katalogów, jak też poszczególnych gałęzi, a nawet, pojedynczych plików.
Przykładowa linia wywołania do szybkiego przeszukiwania dyskietek (bez przeszukiwania pamięci):

SZUKAJ A: /C

Program **SZUKAJ.EXE** można wpisać do pliku AUTOEXEC.BAT, w celu automatycznego przeszukiwania wybranych elementów lub całego dysku.

Oto pełna linia wywołania programu **SZUKAJ.EXE**, z pod DOS'a, łącznie z możliwymi przełącznikami (parametrami):

SZUKAJ.EXE [d:][/auto_del**][**/auto_such**][**/b**][**/batch**][**/c**][**/nomem**][**/alles**][**/still**][**/t@nazwa**][**/help**]**

Opis funkcji przypisanych poszczególnym parametrom programu **SZUKAJ.EXE**

parametr	**przypisana funkcja**
/auto_del	Usuwa wirusy automatycznie (nie zalecamy przy pierwszym przeszukiwaniu pliku!). Nieznany lub zmutowany wirus, który nie mógł zostać usunięty z zachowaniem pliku w którym występował, zostanie automatycznie usunięty razem z plikiem. - **Niebezpieczeństwo utraty plików**.
/auto_such	Szukanie bez usuwania, z utworzeniem protokołu, który może być zapisany w odrębnym pliku lub bezpośrednio wydrukowany

/auto_such [nazwa_pliku] > PRN

/c	*Wyłączenie poszukiwań w pamięci.*
/b	Szukanie wirusów w pamięci poprzez zastosowanie tzw. ´am I there Calls´ - nie jest jednak kompatybilne z każdym PC'tem.
/batch	Pokazuje zdefiniowaną wartość podczas inwazji wirusa(ów) i powoduje, że **SZUKAJ.EXE** kończony pracę zwracając określone wartości ERRORLEVEL.

Przykład:

```
SZUKAJ C:\DOS   /BATCH   >NUL
IF ERRORLEVEL 1 GOTO NIE_WIR
ECHO Uwaga! Nieznane mutacje !!!
GOTO END
:NIE_WIR
.
.
:END
```

Lista z wartościami ERRORLEVEL znajduje się w pliku AVK.TXT.

/nomem Wyłącza przeszukiwanie pamięci.

/help [/?] Pomoc do pliku SZUKAJ.EXE.

/alles Przeszukuje każdy rodzaj pliku (bez podania tego parametru zostaną przeszukane tylko niektóre, standartowo określone pliki).

/STILL Nie ukaże żadnego komunikatu, dopóki program nie znajdzie wirusa.

/t Znaki wpisane po literze "t" zostaną ukazane, na ekranie monitora, w momencie znalezienia wirusa.

/t@nazwa Plik "nazwa" zostanie ukazany na ekranie , w momencie znalezienia wirusa (plik ten musi być plikiem typu TXT i może zawierać maksymalnie 4.000 bajtów).

Przykłady: **SZUKAJ C:\DOS /still**
(Przeszuka C:\DOS. Komunikat zostanie ukazany tylko w przypadku inwazji wirusa(ów).)

C:\AVK5\AVKWIN.EXE /c
(Przeszuka plik AVKWIN.EXE w gałęzi C:\AVK5 bez poszukiwania w pamięci komputera.)

SZUKAJ A: /c /auto_such > REPORT.TXT
(Przeszuka A:\, bez poszukiwania w pamięci, bez usuwania wirusów, raport będzie zapisany w pliku REPORT.TXT)

SZUKAJ A: /alles /still
(Przeszuka A:\, wszystkie pliki - także tekstowe czy graficzne! Komunikat zostanie ukazany tylko w przypadku inwazji wirusa(ów).

Program **SZUKAJ.EXE** można, za pomocą wielu parametrów, dopasować do indywidualnych Państwa potrzeb i umieścić np. w AUTOEXEC.BAT, w celu automatyzacji pewnych operacji.

Kolejność wszystkich parametrów oprócz parametru **[**/t**]** jest dowolna. Parametr **[**/t**]** musi stać zawsze na końcu, gdyż znaki, wpisywane po nim, będą uznane jako tekst i zostaną wyświetlone na ekranie monitora! Gdy chcesz utworzyć plik z raportem (np. REPORT.TXT) nie należy używać razem parametrów **[**/auto_such**]** oraz **[**/t**]**.

Wersja DOS programu

Wersja DOS posiada przyjemną szatę graficzną programu **AntiVirenKit5**, która umożliwia łatwą obsługę i nie wymaga osobnego wprowadzenia. Otwarcie programu **AVK5** dla DOS następuje po wydaniu polecenia:

AVK

Za pomocą licznych parametrów, możemy sterować programem, w dowolny sposób. Istnieje jednak możliwość otwarcia programu z określonymi parametrami jn:

AVK.EXE [/parametr1**] [**/parametr2**][**/etc**]**

(Są akceptowane zarówno małe jak i duże litery.)

Opis funkcji przypisanych poszczególnym parametrom programu **AVK.EXE**

parametr	**przypisana funkcja**
/b	Szukanie wirusów w pamięci poprzez zastosowanie tzw. ´ I am there Calls´.
/col1 /col2 /col3	Zmiany ustawienia kolorów. Bardzo przydatne przy notebookach oraz monitorach monochromatycznych.
/esc	Pozwoli przerwać program przez naciśnięcie klawisza ESC.
/herc	Przystosowuje program do karty Hercules.
/nomem	Wyłącza przeszukiwanie pamięci komputera.
/no_save	Nie zapisuje ustawień parametrów programu.
/v, /vga	Włącza moduł graficzny VGA.
/nobeep	Przy inwazji wirusa(ów) nie będzie wydany ton ostrzegawczy.
/no_alert	Nie zostanie wyświetlony komunikat o powodzeniu usunięcia wirusa.
/rw_error	Funkcja sieciowa. Zapobiega przed błędem dostępu, w sytuacji gdy dany plik, który chcesz przeszukać, jest w użyciu przez innego użytkownika w sieci.

Startowanie komputera z dyskietki

Bardzo często dzwonią do naszego serwisu klienci z następującym problemem: Komputer ma wirusa w sektorze startującym twardego dysku. Również dyskietki są zainfekowane. Aby móc "zbadać" komputer potrzebna jest, wolna od wirusów, dyskietka systemowa DOS'a.

Jest zalecane sporządzenie takiej dyskietki, zaraz po instalacji programu **AVK5**.

Tylko w przypadku, gdy komputer uruchomiony zostanie z "czystej" (od wirusów) dyskietki systemowej to można być pewnym, że komputer nie posiada wirusa w pamięci RAM.

Tak długo, jak znajduje się wirus w pamięci komputera, tak długo nie jest możliwe przeszukiwanie i usuwanie wirusa(ów) z systemu. Przy tzw. Stealth Viren, wirus występujący w pamięci komputera może spowodować, że infekcja tym wirusem pozostanie niezauważona przez program antywirusowy i po przeszukaniu systemu nie zostanie zgłoszone występowanie jakichkolwiek wirusów. Z tego też powodu jest bardzo ważne, żeby jeszcze przed infekcją wirusami, przygotować dyskietka systemowa DOS'a.

Aby sporządzić dyskietkę systemową DOS'a, należy:

1. Uruchomić komputer z oryginalnej dyskietki, z systemem operacyjnym DOS. Dyskietka ta musi być zabezpieczona przed zapisem. (Należy pamiętać, ażeby instalować tą wersję DOS'a, która już wcześniej została zainstalowana!).

2. Odnajdujemy, na dyskietkach instalacyjnych, polecenie FORMAT. Polecenie to znajduje się w zależności od wersji DOS'a na różnych dyskietkach instalacyjnych i nie jest spakowane. Po znalezieniu tego polecenia wpisujemy:

A:\FORMAT A: /S

Po pojawieniu się, stosownych komunikatów o zamianie dyskietek (w napędzie), wykonujemy je i formatujemy dyskietkę, z jednoczesnym zapisaniem plików systemowych.

3. Jeżeli używają Państwo wersji MS-DOS 6.0, 6.2 lub 6.22, to wszystkie polecenia znajdują się na dyskietkach instalacyjnych w formie spakowanej. Dlatego konieczne jest wcześniejsze zainstalowanie systemu na dysku twardym (lub ostatecznie ? dyskietkach). Bardzo pomocne będą wskazówki z podręcznika MS-DOS'a.

   W każdym wypadku komputer winien być uruchomiony z oryginalnej (lub oryginalnie sporządzonej) dyskietki z systemem DOS, o takim samym numerze wersji, jak w komputerze! W ten sposób unika się "przenikania" wirusa do pamięci RAM komputera. Nigdy nie należy używać polecenia FORMAT, które znajduje się na dysku twardym, gdyż istnieje duże prawdopodobieństwo (w przypadku infekcji), że program uruchamiany tym poleceniem posiada wirusa!

4. Na "naszą" dyskietkę systemową należy skopiować nw. polecenia (ze środowiska DOS): MOUSE.COM; HIMEM.SYS; EMM386.EXE; KEYBOARD.SYS; KEYB.COM; DOSKEY.COM

5. Skopiować też należy, z oryginalnej dyskietki z programem **AVK5,** polecenia: **SZUKAJ.EXE**, **AVK.EXE** i **AVKWIN.EXE**.

6. W razie potrzeby (np. jeżeli używamy pamięci rozszerzonej typu extended lub expanded) powinniśmy utworzyć plik CONFIG.SYS i wpisać do niego (miedzy innymi) polecenia instalacyjne dla HIMEM.SYS oraz EMM386.EXE.

7. W razie potrzeby, należy utworzyć także, plik AUTOEXEC.BAT i wpisać do niego te polecenia, które są nam niezbędne do normalnego funkcjonowania systemu np. MOUSE.COM; KEYB.COM

KEYBOARD.SYS;

8. Po dokonaniu powyższych operacji, należy bezwzględnie zabezpiecz dyskietkę przed zapisem!

9. Dyskietkę tą powinno się przechowywać łącznie z oryginalną dyskietką programu **AVK5** .

Przy każdym podejrzeniu inwazji wirusów oraz podczas instalacji nowej wersji programu **AVK5** (aktualizacja programu) należy skorzystać ze sporządzonej dyskietki startowej, wg. kolejności:
- uruchomić komputer ze sporządzonej dyskietki systemowej
- z oryginalnej dyskietki startowej, z najnowszą wersję programu **AntiVirenKit5**, wybieramy polecenie **SZUKAJ.EXE** (jest on zawsze na ostatniej dyskietce instalacyjnym.

SZUKAJ C: /c

Jeśli posiadamy więcej dysków logicznych niż jeden, to należy w miejsce C: wpisywać kolejne dyski, w poszukiwania wirusów.

Innym sposobem przeszukiwania twardego dysku na istnienie wirusów jest skorzystanie z programu AVKWIN.EXE, który to pracuje wyłącznie w środowisku Windows.

W przypadku gdy podejrzewacie Państwo infekcję wirusami, a program **SZUKAJ** nie znalazł żadnego wirusa, zalecamy utworzenie podczas przeszukiwania twardego dysku dodatkowego pliku z protokołem szukania (PLIK REFERENCJI) z opisem wszystkich przeanalizowanych plików. Jest to możliwe tylko przy użyciu programu **AVKWIN** dla wersji Windows.

Następnie po paru godzinach pracy z komputerem , przy otwieraniu i zamykaniu różnych programów, ponawiamy próbę na infekcję.

Wymagania sprzętowe i programowe

Wersję WIndows'ową programu **AVK5**, można zainstalować na wszystkich komputerach kompatybilnych z IBM PC (80286 do Pentium) z zainstalowanym WINDOWS'em od wersji 3.1. Państwa komputer powinien mieć przynajmniej 2MB pamięci operacyjnej (najlepiej 4MB i więcej), aby oprócz Windows, mogły także pracować inne rezydentne programy (np: SmartDrive, RamDisk, itp.).

Numer seryjny programu

Prosimy o podanie numeru wersji, Państwa programu **AVK5 -** przy każdym pytaniu o niego. Jest on wskazówką, o aktualnie posiadanej wersji i umożliwia, przy ewentualnych problemach, udzielenie szybkiej pomocy. Numer wersji znajduje się, w lewym dolnym rogu **głównego okna AVK5** lub wybierając, z menu ***Pomoc,*** polecenie ***Informacja***, a także w nazwie na oryginalnej dyskietce **AVK5.**

Główne okno programu AVK5

Na ekranie Państwa monitora, widoczny jest obraz podobny do znanego z Windows; Menedżera plików. Pasek menu służy do szybkiego wyboru najważniejszych funkcji, selekcji stacji dysków i ich zasobów. Oba okna umożliwiają szybkie przeglądanie struktury dysku (drzewa) i przedstawiają wszelkie zachodzące zmiany, np. nowe pliki itp...

Używane są następujące symbole:


otwarty katalog


zamknięty katalog


plik


rekord startujący (Bootsektor)


pierwszy wyższy poziom w drzewie katalogów

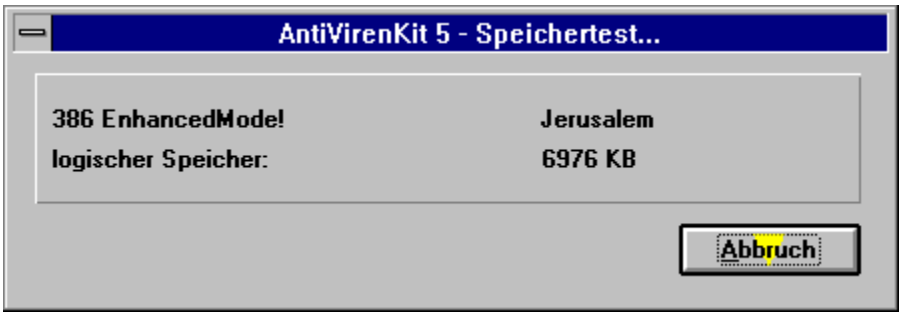
Sterowanie programu

Wszystkie polecenia wybieramy przy pomocy klawiatury albo myszy. Obsługa kombinacji klawiszy (klawisze skrótu) jest adekwatna jak w Windows. W rozwijanym menu podkreślone są litery, których używacie Państwo, w połączeniu z klawiszem ***Alt***. Dodatkowo, liczne polecenia, można wybierać przy pomocy klawiszy funkcyjnych, opisanych za każdym rozkazem obok polecenia. Do sterowania, w rozwijanym menu, można używać także *klawiszy* ***sterujących kursorem*** i klawisza ***Enter*** do zatwierdzania. W polach wyboru używamy klawiszy ***TAB*** i ***Shift-TAB***. Wybrane opcje zostaną otoczone ramką. Więcej informacji dotyczącej obsługi Windows, przy pomocy myszy, znajdziecie Państwo w WINDOWS-MANUAL i w rozwijanej pomocy okienkowej.

Klawisze funkcyjne:

F2	= Analiza stacji dysków
F3	= Analiza automatyczna
F4	= Zaznaczanie jako wyjątek
F5	= Informacje referencyjne
F6	= Usuwanie wirusa
F7	= Kasowanie pliku
F8	= Kopiowanie pliku
Shift + F2	= Kopiowanie katalogu
Ctrl + A...Z	= Wybór dysków A...Z
+	= Podświetlanie gałęzi
-	= Wygaszanie gałęzi

Test pamięci



Po wywołaniu **AVK5**, zostanie najpierw sprawdzona pamięć - czy nie występują w niej już wirusy. Polecamy dodatkowo, przy każdej nowej instalacji, względnie instalacji UpGrade'u, wykonanie szybkiej analizy antywirusowej pamięci RAM.

W trybie standardowym Windows, zostanie zbadana cała pamięć operacyjna, tzw. czysta pamięć RAM - następuje to bardzo szybko.

W trybie 386 (rozszerzonym) zostaną zbadane wszystkie liniowe adresy obszaru Windows. To może być znacznie więcej niż fizyczna pamięć (magazynowane pliki i fizyczne miejsca pamięci z wieloma liniowymi adresami). W tym przypadku nie tylko pamięć RAM, lecz także pamięć na dysku twardym zostanie przeszukana i dlatego ten test, przy dużej ilości plików, może trwać znacznie dłużej. Sprawdzanie pamięci można przerwać w każdym momencie poleceniem ***Anuluj***.

Przy instalacji programu **AVK5** nastąpi modyfikacja pliku SYSTEM.INI o linię wywołania programu AVKWIN.386 (przeprowadzającego ww. test).

SYSTEM.INI:

```
[386Enh]
.........
device= dysk:\...\avkwin.386
.........
```

Lista stacji dysków

Tu przedstawiono symbolicznie istniejące stacje dysków, gdzie obok charakterystycznego symbolu, stacji dysku, przyporządkowana jest mu litera.
Symbolem stacji dysków elastycznych jest 'otwór' w stacji dysków (vide 'A' i 'B'), dla dysków twardych i logicznych 'poziome kreski' (vide jak 'C'), dla stacji dysków CD-ROM krążkiem (patrz jak 'D'), a dla sieciowych stacji dysków przez 'połączenia sieciowe' (jak np. 'M'-'S').
W przypadku, gdy posiadacie Państwo więcej stacji dysków, niż te zawarte w liście, wtedy wyświetlą się (z prawej strony listy), dwie strzałki skierowane w prawo - lewo. Za pomocą tych strzałek istnieje możliwość przewijania listy stacji dysków. Wybór dysków odbywa się przez kliknięcie myszą lub poprzez wybór kombinacji klawiszy ***Ctrl +*** (litera odpowiedniego dysku); np. ***Ctrl + C***. Wybrane stacje dysków przedstawione są w ciemniejszych kolorach. Wybrana stacja dysku otrzyma oprócz tego bezpośrednie połączenie do leżących pod nią list katalogów i plików. Po wyborze stacji dysków mamy możliwość zobaczenia ostatecznego stanu przeprowadzonej analizy.

.

Wybór dysku

Inną możliwością wyboru dysku, jest jego określenie z pola ekranu głównego **AVK5**, umieszczonego ponad symbolami dysków. Kliknięcie w to pole spowoduje wyświetlenie listy dysków, z odpowiadającymi im nazwami (jeśli występują). Jeżeli na pokazanie wszystkich Państwa dysków brakuje miejsca (w oknie), to z prawej strony okna pojawi się pasek przewijania, który służy do pokazywania dalszej części listy. Kliknięcie myszą powoduje wybór odpowiedniego dysku.

Drzewo katalogów / Lista plików

Z lewej strony widzimy strukturę katalogów, inaczej mówiąc, drzewo wybranej stacji dysków. Państwu jest już znana, ta przejrzysta forma przedstawiania zawartości dysku twardego, uzyskana poleceniem TREE w DOS'ie lub w WINDOWS'ie - okno Menedżera plików. Kliknięcie na dowolny katalog oznacza jego wybór. Z prawej strony wyświetla się zawartość katalogu, również podkatalogi i pliki należące do wybranego katalogu. - Są przedstawione, tylko ostatnio sprawdzone pliki. Jeżeli jeszcze nie przeprowadzaliście Państwo analizy, to żadnych plików nie będzie można zobaczyć. Zasadniczo są pokazywane tylko analizowane pliki, które są także uzależnione od wybranych opcji analizy (najczęściej są to pliki wykonywalne, np: *.**COM**, ***.EXE** lub ***.SYS**). Podwójne kliknięcie na katalog, w lewej części ekranu, podświetla automatycznie znajdujące się podkatalogi w liście. Plików nigdy nie zobaczymy z lewej strony. Pliki katalogu będą pokazane zawsze w oknie '*znane / sprawdzone*' pliki. Dwukrotne kliknięcie na katalog w tym oknie, ukaże następną płaszczyznę z plikami i podkatalogami.

Szerokość tych dwóch głównych okien zmienia się przez przesunięcie środkowej, rozdzielającej linii. Proszę wskazać myszą - środkową linię. Gdy kursor zmieni kształt, proszę przeciągnąć linię w wybranym kierunku.

Pasek statusu

Pasek statusu zawsze pokazuje na początku: numer bieżącej wersji programu **AVK5**.
Ta informacja jest bardzo ważna, w przypadku wszelkich pytań, składanych poprzez tzw. Gorącą Linię, do:

LTP MediaSoftware - G DATA Software Sp. z o.o.
78-400 SZCZECINEK

Tel. 0_966-42330
Fax. 0_966-42333

Poza tym, każdorazowo będzie pokazany, dla wybranego katalogu jego status (odwołanie do ... -(*wersja)* **AVK5**, z którą to odwołanie zostało zrobione) i status przy wybranych plikach.

Pasek statusów jest ważną pomocą przy używaniu listy funkcji. Jak tylko wskażemy myszą na dowolny symbol w liście funkcji (bez klikania), względnie wskażemy za pomocą klawiatury, w rozwijanym menu, wybrane pole wyświetli się w pasku statusów w postaci zrozumiałego tekstu.

Lista funkcji

Lista funkcji zawiera najważniejsze funkcje, niezbędne do codziennej pracy z **AVK5**.

= Wybór dysku


= Szukanie wirusa w aktywnej stacji dysku


= Szukanie wirusa w aktywnym katalogu


= Automatyczne szukanie wirusów


= Zaznaczanie katalogu jako wyjątkowy


= Pokazanie plików referencyjnych


= Usuwanie wirusa


= Kasowanie pliku


= Kopiowanie pliku


= Sortowanie listy plików wg ich nazwy


= Sortowanie listy plików wg rozszerzenia ich nazwy


= Sortowanie listy plików wg ich wielkości


= Sortowanie listy plików wg daty ich powstania


= Korzystanie z pomocy


= Lista wirusów

Funkcje, które są niedostępne (w danej chwili) i nie mogą być wybrane, będą przedstawione w jasnoszarym kolorze.

Szukanie wirusów na wybranym dysku

Wybrany dysk będzie cały przeszukiwany. Również będzie przeprowadzona analiza referencyjna. Gdy analiza jest wykonywana po raz pierwszy, to **AVK5** tworzy tzw. plik referencyjny.
Pliki referencyjne będą zapamiętane, w katalogu Windows'a. Dla każdej zbadanej stacji dysku będzie utworzony odrębny plik referencyjny. Plik otrzyma nazwę **AVKREFxx.DAT**. Gdzie '**xx**' oznacza nazwę stacji dysku, która otrzyma przyporządkowany jej kolejny numer (**2**=dysk '**C**', **3**=dysk '**D**' itd...).
Jako kryterium sprawdzania w plikach referencyjnych, będą dla każdego pliku zarejestrowane: data, czas, wielkość oraz różnorodne sumy kontrolne. Taki referencyjny plik tworzy podstawową bazę, w celu ustalenia zmian w badanych plikach. Gdy w systemie próbuje zagnieździć się wirus, to zostanie to natychmiast wychwycone - zmiany występujące w kryteriach podczas sprawdzania. Przy każdym dalszym sprawdzaniu poprzednio zbadanych już plików, będą porównywane aktualne dane statusowe z określonymi kryteriami sprawdzania, z danymi wcześniej zapamiętanymi w plikach referencyjnych. Każda zmiana zostanie natychmiast zauważona.

Stałe pliki referencyjne, będą założone, tylko dla stałych dysków. Wymienne nośniki (dyskietki, CD-ROM'y) otrzymują, w pamięci operacyjnej tylko tzw. czasowe pliki referencyjne, które po zakończeniu pracy **AVK5**, zostaną usunięte.

Szukanie wirusów w wybranym katalogu

Aktualnie wybrany katalog zostanie sprawdzony pod względem występowania wirusów. Równocześnie zostanie przeprowadzona analiza referencyjna wewnątrz tego katalogu. O ile analiza jest robiona pierwszy raz, to **AVK5** tworzy tzw. plik referencyjny (w katalogu Windows'a).
Jako kryterium sprawdzania w plikach referencyjnych, będą dla każdego pliku zarejestrowane: data, czas, wielkość oraz różnorodne sumy kontrolne. Taki referencyjny plik tworzy podstawową bazę, w celu ustalenia zmian w badanych plikach. Gdy w systemie próbuje zagnieździć się wirus, to zostanie to natychmiast wychwycone - zmiany występujące w kryteriach podczas sprawdzania. Przy każdym dalszym sprawdzaniu poprzednio zbadanych już plików, będą porównywane aktualne dane statusowe z określonymi kryteriami sprawdzania, z danymi wcześniej zapamiętanymi w plikach referencyjnych. Każda zmiana zostanie natychmiast zauważona.

Automatyczne szukanie wirusów

Po wykonaniu tej funkcji, wyświetli się pole wyboru, w którym możecie Państwo, określić dyski przeznaczone do zbadania.

Z lewej strony będą pokazane dyski, które nie będą analizowane, a z prawej strony te, które będą podlegały badaniu. Poprzez pojedyncze kliknięcie, można każdorazowo zaznaczyć dowolną ilość stacji dysków na jednej stronie i przesunąć je na drugą stronę.
Poprzez przycisk ***START***, zostaną zbadane pod względem zawartości wirusów, wszystkie wcześniej wybrane dyski. Równocześnie, dla tych dysków, zostanie przeprowadzona analiza referencyjna. Gdy analiza jest wykonywana po raz pierwszy , to **AVK5** tworzy tzw. pliki referencyjne.
Pliki referencyjne zostaną zapamiętane w katalogu Windows'a. Dla każdej zbadanej stacji dysku, będzie utworzony własny plik referencyjny. Plik przyjmuje nazwę **AVKREFxx.DAT**. Gdzie '**xx**' oznacza nazwę stacji dysku, która otrzyma przyporządkowany jej numer (**0**=dyskietka '**A**', **1**=dyskietka '**B**', **2**=dysk '**C**', **3**=dysk '**D**', itd...).
Jako kryterium sprawdzania w plikach referencyjnych, będą dla każdego pliku zarejestrowane: data, czas, wielkość oraz różnorodne sumy kontrolne. Taki referencyjny plik tworzy podstawową bazę, w celu ustalenia zmian w badanych plikach. Gdy w systemie próbuje zagnieździć się wirus, to zostanie to natychmiast wychwycone - zmiany występujące w kryteriach podczas sprawdzania. Przy każdym dalszym sprawdzaniu poprzednio zbadanych już plików, będą porównywane aktualne dane statusowe z określonymi kryteriami sprawdzania, z danymi wcześniej zapamiętanymi w plikach referencyjnych. Każda zmiana zostanie natychmiast zauważona.

Stałe pliki referencyjne, będą założone, tylko dla stałych stacji dysków. Wymienne nośniki (dyskietki, CD-ROM'y) otrzymują, w pamięci operacyjnej tylko tzw. czasowe pliki referencyjne, które po zakończeniu pracy **AVK5,** zostaną usunięte.

Zaznaczenie katalogu jako wyjątek

Kliknięcie na ten symbol, zaznacza wybrany katalog lub wybrany plik jako wyjątek. Tak zaznaczone pliki lub katalogi będą przedstawione w symbolu pliku lub w symbolu katalogu, w postaci ukośnych, zielonych kresek.

Te wyjątkowe katalogi lub pliki nie będą brały udziału w sprawdzaniu na występowanie wirusów i w szukaniu referencyjnym. Jeżeli katalogi te zawierają w sobie podkatalogi, to również i one nie będą sprawdzane. Dowolną ilość plików i katalogów można wyłączyć z przeszukiwania. Powtórne kliknięcie na symbol wyjątku, znosi wcześniej wybraną funkcję i wtedy, poprzednio zaznaczone pliki i katalogi, wezmą udział w sprawdzaniu.
Opcja ta jest szczególnie przeznaczona dla programistów, którzy chcą opracowywane programy chronić przed uciążliwymi komunikatami, o dokonanych w nich zmianach.

Przez wybiórcze **szukanie wirusów w aktualnym katalogu**, można także sprawdzać te, które zostały oznaczone jako wyjątki.

Wyświetlenie danych referencyjnych pliku

Po selekcji pliku, katalogu lub rekordu startującego (Bootsektor), otrzymają Państwo, przy pomocy tej funkcji, szczegółowy raport o dotychczasowych analizach pliku, katalogu lub rekordu startującego.

Najpierw zostanie podana nazwa i data ostatniego sprawdzania. Poniżej status (stan), a w nim informację, czy plik zawiera wirusa, jeżeli tak, to jakiego wirusa, a także w jakim stanie się ten wirus znajduje. Przy przeobrażających się wirusach, które **AVK5** wprawdzie rozpoznaje, ale nie umie ich usunąć (bez zniszczenia pliku), prosimy zawsze o nadesłanie dyskietki z zainfekowanymi plikami. Tylko w ten sposób możemy przeprowadzić dokładną analizę i umożliwić przy następnym pojawieniu się wirusa, jego 100% usunięcie. - Opcja ***Kopia pliku***.
Jako dodatkowe cechy pliku, zostanie przedstawiona jego wielkość, atrybuty DOS'a, data i czas, jak również wyniki sum kontrolnych.

Usunięcie wirusa z wybranego pliku

Usunięcie wirusa z pliku jest wyłącznie możliwe, gdy DIGILOG jest wyłączony, względnie zabezpieczenie przed zapisem: zarażonego pliku, rekordu startującego (Bootsektora) lub tabeli partycji temu nie przeszkodzi. Zwróć uwagę na warunki ustawienia DIGILOC, względnie DIGILOC-Manual.

Usunięcie wirusów z zarażonych plików lub rekordu startującego, jest zasadniczo możliwe tylko wtedy, gdy wirus jest znany i przeanalizowany przebieg infekcji. Na szczęście, dzisiaj jest to możliwe prawie we wszystkich przypadkach standardowych wirusów. **AVK5** rozpoznaje poprzez wiele stopni zabezpieczeń, czy wirus można usunąć. Jeżeli symbol tej funkcji jest osiągalny (wcześniej wyselekcjonować zarażony plik), można z dużą pewnością uwolnić plik od wirusa.
Jeżeli jednak wirus nie jest znany, lub wciąż się przeobraża, lub powstają mutanty wirusa, lub zniszczył nieodwołalnie Twoje dane źródłowe, to nie pozostaje nic innego jak wywołać polecenie ***kasuj wybrany plik***.

Kasowanie wybranego pliku

Wybrany plik zostanie usunięty (wcześniej wystąpi pytanie, o potwierdzenie zamiaru !) i będziecie Państwo musieli go od nowa założyć (po skasowaniu uszkodzonej wersji). Możliwość skasowania zarażonego pliku i następnie założenie go od nowa, jest bardzo ekonomicznym podejściem do problemu. Nowa instalacja daje gwarancję, że w przyszłości nie wystąpią żadne problemy.
W przypadku nieznanego lub mutującego wirusa, jest zawsze ważne, aby kopię zarażonego lub przypuszczalnie zarażonego pliku przesłać na adres **G DATA / LTP MEDIA SOFTWARE**. Do tego celu służy funkcja ***'kopiowanie wybranego pliku***.

 **Kopiowanie wybranego pliku**

To polecenie ułatwi Państwu zadanie, skopiowania zarażonego pliku. Należy włożyć "czystą" dyskietkę do napędu i uaktywnić tą opcję, i oczywiście wcześniej wybrać, z pola wyboru, odpowiedni napęd dyskowy. Zmiana nazwy pliku nie jest konieczna. Klikając ***OK*** i przesyłając dyskietkę na adres:

LTP MediaSoftware - G DATA Software Sp. z o.o.
78-400 SZCZECINEK

Tel. 0_966-42330
Fax. 0_966-42333

Sortowanie listy plików wg nazwy pliku

W zależności od tego, jak wybraliście Państwo, w rozwijanym menu - sortowanie rosnąco lub malejąco - zobaczymy, w oknie plików pliki posortowane wg nazwy.

 Wybrana funkcja, za każdym razem zostanie oznaczona przez wciśnięty symbol, a odpowiednie polecenie w rozwijanym menu, będzie zaznaczone 'haczykiem'.

Sortowanie listy plików wg rozszerzenia nazwy

W zależności od tego, jak wybraliście Państwo, w rozwijanym menu - sortowanie rosnąco lub malejąco - zobaczymy, w oknie plików posortowane nazwy plików wg rozszerzenia nazwy.

 Wybrana funkcja za każdym razem zostanie oznaczona przez wciśnięty symbol, a odpowiednie polecenie, w rozwijanym menu, będzie zaznaczone 'haczykiem'.

 Sortowanie plików wg wielkości

W zależności od tego, jak wybraliście Państwo, w rozwijanym menu - sortowanie rosnąco lub malejąco - zobaczymy, w oknie plików posortowane nazwy plików wg ich wielkości.

 Wybrana funkcja za każdym razem zostanie oznaczona przez wciśnięty symbol, a odpowiednie polecenie, w rozwijanym menu, będzie zaznaczone 'haczykiem'.

Sortowanie listy plików wg daty

W zależności od tego, jak wybraliście Państwo, w rozwijanym menu - sortowanie rosnąco lub malejąco - zobaczymy, w oknie plików posortowane nazwy plików wg daty.

 Wybrana funkcja za każdym razem zostanie oznaczona przez wciśnięty symbol, a odpowiednie polecenie, w rozwijanym menu, będzie zaznaczone 'haczykiem'.

Korzystanie z pomocy

Przedstawia tekst pomocy do programu **AVK5.** Akurat w tym momencie, czytacie go Państwo !

Wyświetlenie listy wirusów

Tutaj zobaczymy listę najważniejszych wirusów, które w obszarze niemieckojęzycznym powodują 85% infekcji. Dla każdego wirusa, są przypisane informację o drodze rozprzestrzeniania, sposobie przenoszenia, wielkości, typie, miejscu zagnieżdżania się wirusa itp.
Jeżeli po przeprowadzonej analizie, zobaczymy w prawej części, na ekranie monitora, nazwę zainfekowanego pliku, to ukaże się także po wywołaniu tego polecenia, informacja o wirusie, który zaatakował Twój plik.

Wynik analizy

AVK5 po przeprowadzonej analizie przedstawia raport:

Tu zebrane są wszystkie znaczące informacje o analizie.
Sprawdzony dysk lub katalog, wersja **AVK5**, liczba plików, data i czas. Status wskazuje, czy został znaleziony wirus.
W spisie plików widzimy ile plików zostało zarażonych po raz pierwszy, ile poprzez modyfikację, a w ilu wykryto błędy odczytu. Do tego jest dołączona liczba skasowanych, skopiowanych lub pominiętych plików, a także ich ilość całkowita.
Poza tym, widzimy status rekordu startującego. Status każdego pliku rozpoznamy w oknie ***katalogu / pliku***.

Status pliku

Pliki mogą posiadać różne statusy, które **AVK5** wyświetla. Do tego przyporządkowany został każdorazowo symbol pliku z zaznaczoną literą lub znakiem.
Po wykonaniu analizy, pliki wykazują następujące cechy statusowe:


Normalny - Plik został przeanalizowany i nie posiada żadnych osobliwości.


Wyjątek - Plik został wyłączony z analizy.


Nowy - Plik, który pierwszy raz został zbadany, w analizie referencyjnej, i którego status (wielkość, data, czas i sumy kontrolne) został przepisany do pliku referencyjnego.


Zmodyfikowany - Plik, którego aktualny status różni się od statusu zapamiętanego w analizie referencyjnej. O ile przyczyna tych zmian nie jest związana z instalacją nowej wersji lub nie zostały znalezione inne znane przyczyny, istnieje podejrzenie o infekcję wirusową. Proszę zrobić kopię tego pliku i przesłać ją do nas, tj. do LTP MediaSoftware-G DATA Software Sp. z o. o.


Wymazany - Plik, który był zapamiętany w pliku referencyjnym, został skasowany.


Wirus - Plik jest zarażony. Dokładniejsze informacje znajdują się w funkcji **Wyświetlenie wszystkich danych referencyjnych dla pliku** lub w **Analizie wynikowej**.


Błąd odczytu - Plik jest akurat otwarty lub w pracy sieciowej został otwarty przez innego użytkownika sieci.

Wszystkie pliki ze specjalnym statusem 




będą przedstawione w odwrotnym kierunku sortowania.

Drukowanie pliku referencyjnego

Drukowanie pliku referencyjnego wybranego dysku.
Przed rozpoczęciem drukowania pliku referencyjnego, istnieje możliwość ustawienia różnych opcji drukowania.

Jeśli podłączonych jest więcej drukarek, można przydzielić dowolną drukarkę z listy drukarek.
Każda strona może zawierać nagłówek i stopkę, w której można podać nazwę firmy, typ urządzenia itd.
Przy wybraniu opcji ***Drukuj wszystko***, będą wydrukowane wszystkie zbadane pliki z ustalonymi cechami referencyjnymi. Poprzez opcję ***Drukuj wyznaczone pliki***, która znajduje się poniżej, wybierasz tylko te pliki, które powinny być drukowane. Wszystkie oznaczone krzyżykiem typy plików zostaną wydrukowane.
Masz do wyboru: zarażone pliki (), modyfikowane pliki (), nowe pliki () lub skasowane pliki (), pliki z błędem odczytu (), i pliki, w których nie wystąpiły żadne zmiany ().
Poprzez przycisk ***OPCJE*** możesz ustawić inne parametry drukarki.

Opcje DIGILOC

Ten punkt Menu może być wywołany tylko dla komputerów z wbudowaną kartą DIGILOC. Jeżeli ten punkt jest jasnoszary, to jest on dla Ciebie nieosiągalny. Przy wbudowanej karcie DIGILOC wyświetli się następujący obraz:

Zostanie pokazany numer wersji DIGILOC, jak też obszar pamięci (szesnastkowo), który jest zajęty przez DIGILOC'a. Aby ustawić obszar pamięci dla DIGILOC'a, przeczytaj najpierw DIGILOC-Manual.
W następnym polu można włączać / wyłączać komunikaty dla DIGILOC'a podczas ładowania. Godnym polecenia jest włączanie komunikatów, co pozwoli zobaczyć status DIGILOC'a podczas ładowania.
W polu poniżej, można ustawić wszystkie opcje DIGILOC'a, jak też w Setup DIGILOC.

Włączanie i wyłączanie dla:

- Ochrony zapisu tabeli partycji
- Ochrony zapisu DOS'owskiego rekordu startującego
- Ochrony przed fizycznym sformatowaniem
- Ochrony zapisu dla plików programowych (w zależności od "kliknięte" typu)

Przy wszystkich ustawieniach rozpoznacie uaktywnione opcje poprzez znak '**x**' w odpowiednim polu wyboru.

Wszystkie zmiany funkcji DIGILOC mogą być dokonane tylko wtedy, jeśli przełącznik ochrony zapisu (jumper) na karcie DIGILOC jest właściwie ustawiony. Programowe odłączenie od DIGI-LOC'u podczas pracy jest niemożliwe, jak również nie przewidziane ze względów bezpieczeństwa.

Wewnątrz opcji , dla dwóch plików wyświetlanych, można dodatkowo wykluczyć ochronę zapisu. W zasadzie polecamy to dla pliku CONFIG.SYS i dla WIN.COM. CONFIG.SYS często podlega zmianom, natomiast WIN.COM jest modyfikowany przy każdej zmianie rozdzielczości ekranu. Również, jest to godne polecenia dla MODE.COM (jeżeli go używasz).

Opcje analizy

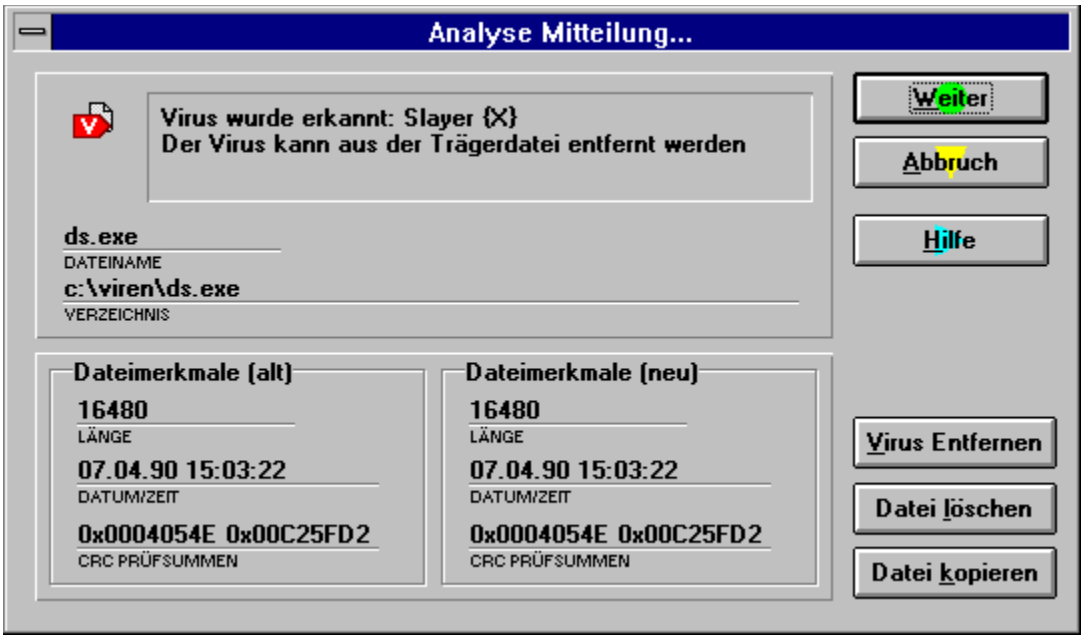
W polu '*Opcje analizy*' można wybrać wszystkie ważne dla analizy opcje.

Wybór 'Badaj wszystkie pliki' jest z reguły bezsensowny, ponieważ wirusy atakują tylko pliki wykonywalne lub sektor ładujący. Ta opcja jest zawarta tylko na życzenie użytkowników i praktycznie jest nie używana - w wielu wypadkach prowadzi do błędnych alarmów związanych z modyfikacją plików tekstowych, graficznych itp.
Istnieje jeszcze inny powód przeciwko wybieraniu tej opcji. Przy bardzo w wielu plikach, gwałtownie zmniejsza się szybkość analizy - utworzone dane referencyjne są olbrzymie. Dla każdego pliku potrzeba 48 bajtów, a dla każdego katalogu potrzeba 256 bajtów. Przykładowo; przy 200 MB na dysku twardym, z 6000 plików i 600 katalogami (przy badaniu wszystkich plików), dane referencyjne uzyskają wielkość ok. 441 600 bajtów.
Dlatego wybór opcji *Badanie wybranych plików* jest lepszy. W polu, poniżej, są uwidocznione wszystkie możliwe wykonywalne pliki. Każdy typ pliku można pojedynczo uaktywnić lub dezaktywować. Dodatkowo można dodać dwa zdefiniowane typy plików.
To ma sens wtedy, gdy plik z rozwinięciem *.PRG został przemianowany na plik z rozwinięciem *.PRX i ten drugi chce się zbadać.

Ważne jest rozstrzygnięcie między opcjami: '*nieprzerwana analiza*' i '*zgłaszanie podczas analizy*'. W pierwszym przypadku będą sprawdzane wszystkie wybrane pliki na badanych dyskach bez wysyłania żadnych komunikatów. W końcu, można pojedynczo kliknąć na zaznaczony plik i w opcji '*Informacja o pliku referencyjnym'* lub przy pomocy klawisza *F6* lub w  liście funkcji wywołać status.
Przy ustawieniu '*Meldowanie podczas analizy'*, możesz dodatkowo ustalić, które komunikaty mogą przerwać analizę. To jest sensowne przy znalezieniu wirusa i przy odkryciu zmian. Dodatkowo wystąpienie nowego pliku powinno być zawsze zgłoszone.

Po starcie następuje wykonanie analizy.

Analizę możesz w każdej chwili przerwać poleceniem *'Anuluj'* . Podczas analizy możesz zawsze ustalić, jakie pliki, w jakich katalogach są aktualnie badane. Poza tym jest podana liczba zbadanych plików, znalezionych wirusów, a również nowych i zmodyfikowanych plików.
Jeśli wybrałeś '*Meldowanie podczas analizy*', to każdy komunikat przerywa wykonywaną analizę.



W tym przykładzie zgłoszenie od analizy zawiera rozpoznany wirus. Później program zgłosi, czy ten wirus zostanie usunięty (bez zniszczenia zainfekowanego pliku).
Jako informacje zostaną zgłoszone nazwa pliku i ścieżka katalogu, jak też cechy szczególne pliku z ostatniej analizy i aktualne, szczególne cechy ostatniej analizy (wielkość, data, czas, jak też sumy kontrolne).
Opcje *'Usuń wirus', 'Kasuj plik' i 'Kopiuj plik'* odpowiadają symbolom listy funkcji. Dodatkowo pojawi się przycisk '*Lista wirusów*', jeśli wirus ten jest w niej zawarty.

Opcje widoku

Wybór '*Opcje widoku*' w rozwijanym menu, zawiera po prawej stronie możliwość ustawienia opcji sortowania plików.

Dodatkowo, po lewej stronie można oznaczyć, które dane przy każdym pliku będą widoczne, a mianowicie: wielkość, data, czas, atrybuty pliku i sumy kontrolne.
Jeśli klikniecie Państwo, na przycisk '*Katalog*', to ukażą się, jeśli istnieją; podkatalogi, a podczas gdy opcja '*Normalne pliki*' daje wgląd w niezainfekowane, niezmienione i nowe pliki.

Wszystkie '*Opcje widoku*' dotyczą tylko prawej strony ekranu monitora.

Katalog wirusów

4096
5120
Anti-Tel
Azusa
Bloody!
Cascade, Cascade-B
Dark Avenger
DIR-2
Flip
FORM-Virus
Hallöchen
Jerusalem
Jerusalem-B
Joshi
Michelangelo
MusicBug
Noint
Parity Boot
Perfume
Ping Pong
Ping Pong-B
PLASTIQUE
PLASTIQUE-B
Slayer Familie
Stoned
Syslock
Telecom
Tequila
USSR 1689
Vacsina
Vienna
W13
Yankee Doodle

5120

ALIAS: Vbasic, Basic Virus
WIELKOŚĆ: 5120
TYP: nierezydentny w pamięci
atakuje pliki COM/EXE
zaraża COMMAND.COM

OBJAWY: Zarażone pliki COM rozrastają się o 5120 B; występują pozornie nieuzasadnione dostępy do twardego dysku; przy próbach zarażenia wirusem, zabezpieczonych przed zapisem plików, występują od DOS'a komunikaty o błędach.

Działanie: **5120** zaraża dowolne pliki COM i EXE. Uruchomienie zarażonego programu prowadzi do tego, że w aktualnym katalogu na aktualnej stacji dysku, dalsze pliki COM i EXE zostaną zarażone; poza tym wybrany wg. algorytmu liczb losowych następny plik COM/EXE zostanie zarażony w każdym katalogu stacji dysku C:.

W następstwie tego zarażenia, mogą ulec zmianie dane, a pliki systemowe DOS'u mogą ulec uszkodzeniu przez błędne przyporządkowanie sektorów.

Poza tym: Ten wirus powstał w skomplikowanym BASIC'u i dlatego , na końcu każdego, zarażonego programu znajdują się takie słowa jak: ´BASRUN´, ´BRUN´, ´IBMBIO.COM´, ´IBMDOS.COM´, ´COMMAND.COM´ oder ´Access denied´.
Jednakże istnieje odmiana tego wirusa bez tych wyżej wymienionych słów.

Anti-Tel

ALIAS: Telecom Boot, Spanish Telecom
WIELKOŚĆ: [-]
TYP: rezyduje w pamięci
zaraża sektor startowy na dyskietkach (Bootsektor)
zaraża tabelę partycji twardego dysku

OBJAWY: Całkowita i dostępna pamięć operacyjna zostanie zredukowana; System-Performance zmniejsza się; fałszowanie danych na twardym dysku.

Działanie: Jeśli system startuje (booten) z dyskietki, która została zarażona wirusem **ANTI-TEL**, to instaluje się wirus rezydentnie w górnym końcu pamięci operacyjnej, ale zawsze poniżej granicy 640KB; program DOS'a pokazuje o 1KB pamięci mniej niż się oczekuje. Wirus **ANTI-TEL** zaraża bezpośrednio z pamięci wszystkie twarde dyski i dyskietki, w których pliki były używane.

Na HD-dyskietkach, zostanie oryginalny Boot-sektor przesunięty do 28 sektora; wirus kopiuje pierwszą część swojego kodu programowego do sektora 0, a resztę do sektora 27. Ponieważ, sektory 27 i 28 należą do głównego katalogu, wszystkie pliki, które posiadają odnośniki do tych sektorów zostaną zniszczone.

Na 360KB-dyskietkach, zostanie oryginalny Boot-sektor na 12 sektor przesunięty; wirus kopiuje pierwszą część swojego kodu programowego do sektora 0 i resztę do sektora 10. Ponieważ sektor 10 i 11 należą do głównego katalogu (wszystkie pliki, które posiadają odnośniki w tych sektorach, zostaną zniszczone).

Na twardym dysku wirus kopiuje swój kod programowy do tabeli partycji twardego dysku i do sektora 6, na stronę 0,do cylindra 0; tabela partycji zostaje przesunięta do 7-go sektora. Ponieważ DOS normalnie tych sektorów nie używa, dane zmagazynowane w tym miejscu przez specjalne oprogramowanie, też ulegną zniszczeniu.

ANTI-TEL należy do grupy zamaskowanych wirusów, które używają aktywnych środków, aby ich odkrycie przez programy szukające nie dało pozytywnego rezultatu; środki kamuflażu wirusa **ANTI-TEL** nie są czysto programowane, i dlatego kamuflaż nie jest skuteczny dla dyskietek, jest jednak skuteczny, jeśli chodzi o twardy dysk.

ANTI-TEL uaktywnia się po 400 ładowaniach systemu i jest niesłychanie destrukcyjny. Ukazuje się wiadomość:

´VIRUS ANTITELEFONICA (BARCELONA)´

i dwa pierwsze dyski twarde zostaną zapisane śmieciami.

WARIANTY: Telecom Boot: Ten wirus występuje przy zarażeniach tabeli partycji wirusem **TELECOM**. Bardzo przypomina on wirus **ANTI-TEL**, jednakże nie zaraża dyskietek.

Azusa

ALIAS: Hong Kong
WIELKOŚĆ: [-]
TYP: rezyduje w pamięci
atakuje sektory startowe
atakuje tabelę partycji twardego dysku

OBJAWY: Zmniejszenie całkowitego i będącego do dyspozycji obszaru pamięci o 1KB; połączenia COM i LPT1 będą sparaliżowane po każdym trzydziestym drugim startowaniu systemu.

DZIAŁANIE: Jak tylko zostanie załadowany system z zarażonej dyskietki startowej, wirus **AZUSA** instaluje się rezydentnie i kopiuje się do tabeli partycji, niszcząc znajdujące się tam dane. Przed wirusem nie ratuje się tabeli partycji. Jeśli wirus jest aktywny, to każde otwarcie pliku do pisania na włożonej dyskietce lub każde startowanie systemu z dyskietki powoduje, że sektor ładowania zostanie na 40 ścieżkę, w sektorze 8 skopiowany, i na miejsce sektora ładowania wpisuje się kopia wirusa; to prowadzi do tego, że dla dyskietek o pojemności większej niż 360KB, kopie sektora ładowania przepisane będą w środek dyskietki, i ewentualnie zapisane tam pliki ulegną zniszczeniu. Przy każdym ładowaniu systemu będzie zwiększał się wewnętrzny licznik wirusa; gdy licznik osiągnie wartość 32, będzie ponownie ustawiony na zero i wtedy też połączenia COM1 i LPT1 będą sparaliżowane. Dla wartości tego licznika od 1 do 31 połączenia COM1 i LPT1 będą pracowały poprawnie.

WARIANTY: **Azusa 2:** Wielkość 2048B, podobieństwo objawów jak przy **AZUSA**, poza tym możliwość złego działania kombinacji klawiszy 'Ctrl + C' i zawieszanie się systemu (w trakcie ładowania go z zainfekowanej dyskietki).

Bloody!

ALIAS: Beijing, Peking
WIELKOŚĆ: [-]
TYP: rezydujący w pamięci
atakuje sektory startowe dyskietek
atakuje tabelę partycji twardego dysku

OBJAWY: Wydłużony czas startowania systemu, zmniejsza całkowity i dostępny obszar pamięci, zgłasza komunikaty na ekranie monitora podczas ładowania systemu, zmienia zawartość sektora ładowania i tabeli partycji twardego dysku.

DZIAŁANIE: **BLOODY**! atakuje sektory ładowania na dyskietkach i tabele partycji na twardych dyskach. Gdy startujesz system przy pomocy zarażonej dyskietki, wirus instaluje się w pamięci rezydentnej pod koniec górnego obszaru pamięci zajmowanej przez DOS, jednak zawsze poniżej granicy 640KB i zmniejsza całkowity, dostępny obszar pamięci o 2KB. Proces ładowania systemu trwa znacznie dłużej niż normalnie. Gdy system nie jest startowany z twardego dysku, natychmiast zostaną zarażone wirusem tabele partycji. Poza tym, przy każdym ładowaniu systemu, zwiększa się wewnętrzny licznik wirusa. Gdy licznik ten osiągnie wartość 128, to podczas ładowania systemu ukaże się komunikat od wirusa następującej treści:

´Bloody! Jun. 4, 1989´

Ta szczególna data nawiązuje do krwawych zamieszek w Pekinie między chińskimi studentami a oddziałami wojskowymi.

Ta wiadomość będzie się ukazywać przy każdym, dalszym 6-tym procesie ładowania systemu. Tekst ten jest zakodowany w wirusie, a więc przy oglądaniu tabeli partycji jest on niewidoczny. Wirus rezydujący w pamięci próbuje zaatakować każdy dysk / dyskietkę, jeśli dokonuje się dowolnej operacji na znajdującym się tu pliku lub programie; rozkaz DIR nie prowadzi jednak do zarażenia (nie wzbudza wirusa).

'Uratowany' sektor ładujący zarażonej 360KB-dyskietki, zostanie zapisany w 11 sektorze, który jest częścią obszaru głównego katalogu; gdy obszar ten był używany, to należące do niego pliki przepadają. Inne typy dyskietek mogą poprzez kopię sektora ładowania stać się nieużyteczne lub będą posiadać zniszczone pliki.

Na twardym dysku sektor ładowania będzie kopiowany (przez wirus) na stronę 0, do cylindra 0, do sektora 6.

Cascade, Cascade-B

ALIAS: Blackjack, 1704, 1704-B, 1701 Family
WIELKOŚĆ: 1704
TYP: rezydujący w pamięci
atakuje pliki COM
wirus łączący się

OBJAWY: Zainfekowane COM-pliki powiększają się o 1704B; nieregularne restartowanie systemu (Warmstart).

DZIAŁANIE: **Cascade**, **Cascade-B** lub **1701**, **1704** należą do najbardziej znanych i rozpowszechnionych wirusów. **Cascade**-wirus jest znany ze specjalnych efektów: spadających liter z ekranu monitora. Jest to pierwszy wirus, który potrafi sam się modyfikować. **Cascade-B** przypomina wirusa **Cascade**, jednakże tu olbrzymi algorytm liter został zastąpiony przez proces restartu (Warmstart), który jest aktywny co pewien przypadkowy czas.

WARIANTY: **1704-C:** Działa jak **1704-B**, jednakże tylko w grudniu każdego roku.

Dark Avenger

ALIAS: Black Avenger, Eddie, Diana, Rabid Avenger,
VAN SOFT, Dark Avenger 1801
WIELKOŚĆ: 1800
TYP: rezydujący w pamięci
atakuje pliki COM, EXE, OVL

OBJAWY: Pliki COM i EXE zostaną powiększone; niszczy pliki i dysk twardy.

DZIAŁANIE: **DARK AVENGER** instaluje się rezydentnie i jest wyjątkowo 'płodny' przy atakowaniu plików programowych, które z jakichkolwiek powodów są otwierane; tak więc przy kopiowaniu rozkazem DOS'a COPY lub XCOPY, oryginalne pliki i powstałe kopie są przez wirus zaatakowane.
Zaatakowane pliki powiększają się o 1800B.

DARK AVENGER jest bardzo podstępny. Wirus wprowadza licznik do sektora ładowania. Po każdym 16-tym zaatakowaniu jakiegoś programu, zostaje wybrany całkiem przypadkowy sektor na dysku twardym, do którego zapisze się część wirusa. Oryginalna zawartość sektora zostaje zniszczona, programy i pliki należące do tego sektora są nie do uratowania.

Wirus zawiera łańcuchy znakowe:

´The dark Avenger, copyright 1988, 1989´, ´This program was written in the city of Sofia. Eddie lives... somewhere in time!´

Chociaż ten wirus jest prawie tak duży jak **JERUSALEM**-wirus, nie wykazuje jednak żadnych podobieństw.

WARIANTY: **Dark Avenger-B:** Jest bardzo podobny do **Dark Avenger**. Różnica polega na tym, że pliki COM będą powtórnie zaatakowane. Wirus ten, inaczej niż oryginał, rezyduje w wyższym obszarze pamięci. Zawarte łańcuchy znakowe zostały lekko zmienione:

´Eddie lives... somewhere in time!´, ´Diana P.´, ´This program was written in the city of Sofia´, ´(C) 1988-1989 Dark Avenger´

Dark Avenger 1801: Jest o jeden bajt dłuższy niż oryginał, rezyduje również w wyższym obszarze pamięci, jednak nie atakuje powtórnie zarażonego już pliku COM.

Rabid Avenger: Bazuje na **Dark Avenger-B**, zajmuje 3696B w górnym obszarze pamięci DOS'a, jednak zawsze poniżej granicy 640KB; zaatakowane pliki będą zwiększone o 1806-1823B; poza tym, wariant ten został tak zmieniony, że nie zostaje rozpoznawany przez znawców wirusów jako wariant **Black Avenger** . Łańcuchy znakowe w wirusie:

´<- Thanks to Dark Avenger ->´, ´Eat us!´, ´(C) 1991 RABID International Development Corp!´, ´Scan String Killer Test´

Van Soft: Odróżnia się od oryginału głównie poprzez teksty, które mają postać(dla drukarki są to znaki niewidoczne):

´V.A.N. Soft & MMMM PRESENT :SOFIA´, ´VAN&MMMM´

Zainfekowane programy COM zostaną zwiększone o 1800B, pliki EXE ulegną zwiększeniu o 1806-1824B; wirus dopisuje się do końca pliku.

Flip

ALIAS: [-]
WIELKOŚĆ: 2343
TYP: rezyduje w pamięci
atakuje pliki COM, EXE, OVL
atakuje sektory startowe dyskietek
atakuje tabelę partycji twardego dysku

OBJAWY: Pliki COM i EXE zostaną powiększone; zmniejsza się całkowity i dostępny obszar pamięci; pojawiają się błędy przyporządkowania plików; sektor ładowania i tabele partycji będą zmienione.

DZIAŁANIE: Startujący plik (zaatakowany) *.EXE przez wirus **FLIP**, wpisuje wirus w górnym obszarze pamięci. Całkowity i będący do dyspozycji obszar pamięci (wg. programu DOS'a CHKDSK.COM) zmniejsza się o 3064B. Poza tym, C:\COMMAND.COM, o ile występuje, będzie zaatakowany; tak długo jak ten wirus jest aktywny w pamięci, zmiany wielkości są niezauważalne. Poza tym dokonują się zmiany w sektorze ładowania w tabeli partycji. Na dyskietkach zmiany wielkości danej COMMAND.COM są dostrzegalne.

Każdy wykonywany program wraz z plikiem nakładkowym (Overlay), będzie zaatakowany.

Zazwyczaj występują błędy przyporządkowania plików, które mogą zniszczyć pliki danych.

Każdego dnia miesiąca, między godziną 16:00 i 16:59, mogą wystąpić na ekranie monitora strony pozamieniane w poziomie, w systemie, który został wystartowany z zarażonego wirusem twardego dysku i który zarządzany jest przez adapter EGA lub VGA.

Wirus nie atakuje żadnych dalszych plików, jeśli został wystartowany z pliku COM lub z sektora ładowania; dalsze przenoszenie wirusa jest możliwe tylko poprzez pliki EXE.

WARIANTY: **Flip-B:** jest trochę mniejszy (2153B) niż oryginał; te warianty rozprzestrzeniają się nie tylko przez pliki EXE, lecz także przez tabele partycji twardego dysku.

FORM-Virus

ALIAS: Form, Form Boot
WIELKOŚĆ: [-]
TYP: rezydujący w pamięci
atakuje sektory startowe dyskietek

OBJAWY: Odgłosy klikania w głośniku komputera.

DZIAŁANIE: Jeśli system po raz pierwszy startowany jest z dyskietki startowej zarażonej wirusem **FROM**, to wirus instaluje się w pamięci i również atakuje sektor startowy na twardym dysku. Proces startowania systemu z zarażonej dyskietki może się nie udać, ponieważ system się zawiesza. W wirusie może się znajdować taki tekst:

´The Form-Virus sends greetings to everyone who´s reading this text. FORM doesn´t destroy data! Don´t panic. Fuckings go to Corinne.´

W zaatakowanym systemie, począwszy od 24-dnia każdego miesiąca, można usłyszeć odgłosy klikania w głośniku komputera.

Tę formę wirusa można w prosty sposób przy pomocy rozkazu DOS'a SYS.COM usunąć (SYS A: C:).

Hallöchen

ALIAS: [-]
WIELKOŚĆ: 2011
TYP: rezydujący w pamięci
wirus łączący się
atakuje pliki COM i EXE

OBJAWY: Zaatakowane pliki COM zwiększają się o 2011-2026B, zaatakowane pliki EXE zwiększają się o 2011-2026B; wprowadzone dane z klawiatury będę fałszowane (nie do rozpoznania).

DZIAŁANIE: **HALLÖCHEN** instaluje się rezydentnie w pamięci, skoro tylko uruchomi się zainfekowany program, chyba, że wielkość zaatakowanego programu przekracza 64KB lub program ten utworzony będzie z datą miesiąca i roku zgodnego z danymi systemu. Wirus powiększa zarażony program do najbliższej całkowitej wielokrotności liczby 16, zanim dopisze on swoją kopię o długości 2011B do zainfekowanego programu. Jeśli wirus będzie aktywny, to wprowadzenia z klawiatury są nie do rozpoznania.

Jerusalem

ALIAS: PLO, Israeli, Friday 13th, Russian, 1813(COM), 1808(EXE)
WIELKOŚĆ: 1813 bzw. 1808
TYP: rezyduje w pamięci
atakuje pliki COM i EXE

OBJAWY: Pliki COM i EXE będą powiększone; efektywność systemu (System performance) zmniejszy się; pliki będą kasowane w każdy piątek 13-tego w miesiącu; pojawi się czarne okno na ekranie monitora.

DZIAŁANIE: **JERUSALEM** odwraca przerwanie nr 8; w 30 minut po wywołaniu zarażonego programu, jego efektywność systemowa wynosi 10% początkowej prędkości programu. Niektóre odmiany pokazują na dole, z lewej strony ekranu czarne okno, które przy korzystaniu z funkcji przewijania ekranu (Scrollen) wędruje do góry ekranu.

13 (trzynastego) wypadającego w piątek, będą kasowane wszystkie wykonywane programy zarażonego systemu.

W niektórych wariantach znajduje się łańcuch tekstowy ´sUMsDos´, jednakże nowsze warianty nie posiadają tego tekstu.

Jerusalem-B

ALIAS: Arab Star, Black Box, Black Window, Hebrew University
WIELKOŚĆ: 1813
TYP: rezyduje w pamięci
atakuje pliki COM, EXE, OVL, SYS.

OBJAWY: Pliki COM i EXE będą powiększone; efektywność systemu zmaleje; pliki będą kasowane każdego trzynastego w piątek w miesiącu; czarne okno na ekranie monitora.

DZIAŁANIE: Wirus **JERUSALEM-B** jest praktycznie identyczny z wirusem **JERUSALEM**, poza tym, że nie występuje wielokrotne zarażenie plików EXE.

JERUSALEM-B jest jednym z najbardziej rozpowszechnionych wirusów.

Nie wszystkie warianty zmieniają efektywność systemu. Wirus staje się aktywny, jeśli o danej dacie, poprzez start zarażonego programu dociera do pamięci. Znajdując się w pamięci, gdy data się zmieniła, nie jest aktywny.

WARIANTY: A-204: Tekst ´sUMsDOs´ został zmieniony na ´*A-204´, kodowanie zostało zmienione, aby zapobiec rozpoznawaniu przez detektywa wirusów (Virenscanner). Ten wariant zmniejsza prędkość systemu i wyświetla na ekranie monitora czarne okno.

Anarkia: Podobnie, jak oryginał, jednakże prędkość systemu będzie bardziej zmniejszona, przy czym czas trwania zmniejszonej prędkości systemu jest znacznie dłuższy. Nie wyświetla się żadne czarne okno; tekst ´sUMsDOs´ będzie zastąpiony przez ´Anarkia´. Ten wariant wirusa staje się aktywny każdego trzynastego wtorku, jeśli wypada on w danym miesiącu.

Anarkia-B: Podobnie jak **Anarkia**, jednakże wirus staje się aktywny zawsze dwunastego października.

Apocalypse: Ten wariant atakuje programy podczas ich wykonywania. Pliki COM rosną o 1808-1822 B przy pierwszej infekcji, przy następnych o 1808 B . Tekst ´MsDos´ będzie zastąpiony przez ´C.J**´. Po 30 minutach w zaatakowanym systemie, ukazuje się charakterystyczne czarne okno. Ten wirus nie kasuje plików.

Captain Trips: Nazwa pochodzi od występującego tu łańcucha znakowego 'Capitan Trips'. W tym wariancie nie wyświetla się żadne czarne okno na ekranie, nie zmniejsza się prędkość systemu i programy nie są kasowane w piątek trzynastego. Pliki COM rozrastają się o 1813B. Pliki EXE rozrastają się o 1808-1822B przy pierwszej infekcji, przy każdej następnej infekcji rozrastają się o 1808B.

Captain Trips 2: Jest to wariant wersji 'Capitan Trips', która została zmieniona po to, aby nie być rozpoznawalną przez Programy wyszukujące wirusy (Virenscanner). Pliki EXE rozrastają się o 1808B.

Jerusalem-C: Podobny do **Jerusalem-B**, jednak z normalnym czasem zmniejszania prędkości systemu.

Jerusalem-D: Wariant **Jerusalem-C**, który w każdy piątek trzynastego po 1990 roku, niszczy obydwie kopie FAT.

Jerusalem-DC: Podobny do **Jerusalem-B**; tekst ´sUMsDOs´ wyspacjowany; po 30 minutach zmniejsza się efektywność systemu o 30% i wyświetla się czarne okno. Ten wariant nie ma żadnej daty pobudzającej go do aktywności.

Jerusalem-E: Wariant **Jerusalem-D**, który w każdy piątek trzynastego, po 1992 roku niszczy obie kopie FAT.

Jerusalem USA: Jak **Jerusalem-C**, kasuje także w piątek, wg. generatora liczb losowych przypadkowe pliki i FAT.

Mendoza: Jak **Jerusalem-B** ale nie atakuje plików EXE. Jest aktywny w miesiącach od lipca do grudnia każdego roku. Każdego dnia istnieje 10%-owa szansa zniszczenia wszystkich aktywnych programów.

Park ESS: Zwalnia system o 20%, czarne okno ukazuje się po 30-tu minutach.

Phenomene: Podobny do wirusa Apocalypse, atakuje także plik COMMAND.COM. Wirus zawiera tekst ´Phenomene.COM´.

Puerto: Podobny do wirusa Mendoza; reinfekuje pliki EXE.

Skism-1: Duże podobieństwo do innych wariantów i oryginału. Jest aktywny od roku 1991-go w każdy piątek, po 15-tym. W tych dniach rozmiary wszystkich aktywnych plików będą skrócone do zera. Rozmiary plików typu COM rosną o 1808, a plików EXE o 1808-1822 bajtów. Wprowadza czarne okno i hamuje pracę systemu.

Spanish JB: Nazywany także ´Jerusalem-F´ lub ´Jerusalem-E2´; nie wprowadza czarnego okna, reinfekuje pliki EXE.

Swiss 1813: Brak czarnego okna, nie usuwa plików, nie zwalnia pracy systemu.

Joshi

ALIAS: Happy Birthday Joshi, Stealth Virus
WIELKOŚĆ: [-]
TYP: rezyduje w pamięci
atakuje sektory startowe dyskietek
atakuje tabelę partycji twardego dysku

OBJAWY: System zawiesza się; komunikat na ekranie monitora.

DZIAŁANIE: Po załadowaniu systemu z dyskietki startowej zarażonej przez wirus **JOSHI**, instaluje się wirus rezydentnie w pamięci i zajmuje około 6KB; podobnie wygląda komunikat rozkazu CHKDSK.COM.

JOSHI wykazuje podobieństwo do dwóch wirusów:
- podobnie, jak wirus **Stoned**, atakuje tabele partycji dysku twardego,
- podobnie, jak wirus **Brain**, pokazuje przy próbie czytania sektora zawierającego tabelę partycji, kopię tego sektora.

5 stycznia każdego roku system nie chce się załadować, towarzyszy temu następujący komunikat na ekranie:

´type Happy Birthday Joshi´

Jeśli użytkownik wprowadzi z klawiatury wyżej wymieniony tekst: ´Happy Birthday Joshi´, może dalej korzystać ze swego systemu.

Jeśli dwa pierwsze bajty sektora startowego dyskietki mają wartość 'EB' i '1F', to znaczy, że dyskietka jest zarażona przez wirus **JOSHI**. Faktyczny kod programowy wirusa znajduje się na 41 ścieżce 360KB dyskietce lub na 81 ścieżce dyskietki 1.2MB.

Te dwie wartości 'EB' i '1F' znajdują się też w sektorze, w którym normalnie zawarta jest tabela partycji twardego dysku. Kopia tabeli partycji znajduje się na ścieżce 0 w 9-tym sektorze.

Michelangelo

ALIAS: [-]
WIELKOŚĆ: [-]
TYP: rezydujący w pamięci
atakuje sektory startowe dyskietek
atakuje tabelę partycji twardego dysku

DZIAŁANIE: **MICHELANGELO** instaluje się rezydentnie w pamięci, jeśli system po raz pierwszy ładowany jest z zarażonej dyskietki, a także wtedy, gdy ładowanie systemu kończy się niepomyślnie. Całkowity i będący do dyspozycji obszar pamięci zmniejsza się o 2KB, które wirus zajmuje w górnym obszarze pamięci, ale zawsze poniżej granicy 640KB. Wirus broni się przed nowym zapisem przez inne programy. Atakuje niezainfekowane dyskietki, gdy tylko ma do nich dostęp; będą zaatakowane tabele partycji na twardym dysku, jeżeli wykonasz dowolne operacje na plikach znajdujących się na tym twardym dysku.

Na 360KB dyskietkach, oryginalny sektor startowy systemu zostanie przeniesiony przez wirus do sektora 11 (ostatni sektor głównego katalogu), a przy dyskietkach 1,2MB na 28 sektor (również do sektora głównego drzewa).Jeżeli sektor ten był przez katalogi wykorzystywany, to zapisane pliki ulegną zniszczeniu.

Sektor z tabelą partycji zostanie przepisany przez wirus do sektora 7, na ścieżkę 0, do cylindra 0.

Wirus przystępuje do ataku 6-go marca, gdzie cały dysk twardy zostanie zapisany przez zawartość pamięci operacyjnej.

W swojej konstrukcji jest ten wirus podobny do wirusa Stoned.

MusicBug

ALIAS: Music Boot, Music Bug
WIELKOŚĆ: [-]
TYP: rezyduje w pamięci
atakuje sektory startowe dyskietek
atakuje tabelę partycji twardego dysku

OBJAWY: Zmniejszenie całkowitego i dostępnego obszaru pamięci; odgłosy klikania; zniszczone obszary na dysku twardym; samowolna muzyka.

DZIAŁANIE: **MUSIC BUG** instaluje się rezydentnie w pamięci, gdy system ładuje się pierwszy raz z zarażonej dyskietki startowej. Całkowity i będący do dyspozycji obszar pamięci zmniejsza się o 2KB, które wirus zajmuje w górnym obszarze pamięci, ale zawsze poniżej granicy 640KB. Wirus broni się przed nowym zapisem przez inne programy. Podczas ładowania systemu z zarażonej dyskietki / dysku twardego, mogą wystąpić odgłosy klikania w głośniku komputera, jednakże częściej mogą to być krótkie kawałki melodii.

Jeśli wirus zainstalował się rezydentnie w pamięci, to przy każdym korzystaniu z dyskietki / dysku twardego usłyszysz dalsze części melodii. Poza tym każda dyskietka / dysk twardy zostanie zaatakowany, jeżeli będzie użyty. Na dysku twardym będzie zarażony sektor startowy i tabela partycji. Poza tym program DOS'a CHKDSK wykazuje 4096B w straconych obszarach, które zawierają wirusa i kopię oryginalnego sektora ładowania; w tych 4096B znajduje się między innymi następujący tekst:

´MusicBug v1.06. Macrosoft Corp.´, ´Made in Taiwan´

Noint

ALIAS: Bloomington, LastDirSect
WIELKOŚĆ: [-]
TYP: rezyduje w pamięci, ukryty
atakuje sektory startowe dyskietek
atakuje tabelę partycji twardego dysku

OBJAWY: Całkowity i dostępny obszar pamięci będzie zredukowany; katalogi będą zniszczone.

DZIAŁANIE: **NOINT** ładuje się rezydentnie do pamięci, gdy system jest startowany po raz pierwszy z zainfekowanej dyskietki. Całkowita i dostępna pamięć zostanie o 2KB zmniejszona, którą wirus zajmuje dla siebie pod koniec górnego obszaru pamięci, jednakże zawsze poniżej granicy 640KB. Po tym czasie tabela partycji będzie już zaatakowana.

Sektor tabeli partycji zostanie przepisany do sektora 7, na stronę 0, do cylindra 0.

Dla dyskietek 360KB będzie przez wirus przepisany oryginalny sektor ładowania do sektora 11 (ostatni sektor głównego katalogu), a dla dyskietek 1.2MB na sektor 17 (również do głównego katalogu). Jeżeli były te sektory rzeczywiście przez katalogi wykorzystywane, to odpowiednie pliki ulegną zniszczeniu. Wirus **NOINT** nie daje żadnych komunikatów przy startowaniu systemu; dostęp do systemu /dysku twardego oraz proces startowania systemu trwa znacznie dłużej niż przy nie zainfekowanym systemie. Ładowanie systemu z nie zarażonej dyskietki startowej 1.2MB, często bywa przerywane z powodu błędu ładowania systemu.

Perfume

ALIAS: 765, 4711, G-Virus
WIELKOŚĆ: 765
TYP: atakuje pliki COM

OBJAWY: Pliki COM rozrastają się - na ekranie monitora komunikat.

DZIAŁANIE: PERFUME atakuje tylko pliki COM, a szczególnie szuka COMMAND.COM, aby ten plik zainfekować. Wirus czasami zadaje pytanie w czasie uruchamiania zainfekowanego programu i startuje ten program, jeśli na to pytanie otrzyma odpowiedź '4711'. Istnieje szeroko rozpowszechniona wersja tego wirusa, gdzie pytania zostały zapisane przez zupełnie przypadkowe liczby.

Ping Pong

ALIAS: Bouncing Ball, Bouncing Dot, Italian, Vera Cruz
WIELKOŚĆ: [-]
TYP: rezyduje w pamięci
atakuje sektory startowe dyskietek

OBJAWY: Gry na ekranie monitora.

DZIAŁANIE: Jeśli **PING PONG** uaktywnia się (wg. algorytmu liczb losowych), wyświetla się na ekranie monitora piłka podskakująca w koło, która może być usunięta tylko przez nowe załadowanie systemu. Inne szkody nie są znane.

Oryginalny wirus atakuje tylko dyskietki.

Ping Pong-B

ALIAS: Bouncing Ball Boot, Italian-A
WIELKOŚĆ: [-]
TYP: rezyduje w pamięci
atakuje sektory startowe dyskietek

OBJAWY: Gry na ekranie monitora.

DZIAŁANIE: **PING PONG-B** jest odmianą wirusa **PING PONG**; główna różnica polega na tym, że **PING PONG-B** atakuje także twardy dysk. Wirus ten, podobnie jak wirus FROM może zostać usunięty rozkazem DOS'a SYS (również PING PONG-C).

WARIANTY: **PING PONG-C:** Podobny do **PING PONG-B**, jednakże bez grafiki.

PLASTIQUE

ALIAS: Plastic Bomb, Plastique 3012, Plastique 1, Anticad
WIELKOŚĆ: 3012
TYP: rezyduje w pamięci
wirus łączący się
atakuje sektory startowe dyskietek
atakuje pliki COM i EXE
nie atakuje COMMAND.COM

OBJAWY: Działanie wirusa jest zależne od daty systemu; zainfekowane pliki COM i EXE zwiększają się o 3012-3020B; nie poraża sektorów startowych dyskietek; odgłosy eksplozji w głośniku komputera; efektywność systemu pozornie maleje.

DZIAŁANIE: Przy pierwszym starcie porażonego programu, instaluje się PLASTIQUE rezydentnie w pamięci i zajmuje przy tym 3264B w dolnym obszarze pamięci. Wirus próbuje każdy plik COM/EXE, który jest wykonywany lub tylko otwierany, zarazić; zainfekowane pliki COM rozrastają się o 3012B, pliki EXE o 3020B.

Jeżeli data systemu jest większa od 20.9 danego roku, wtedy wirus jest złośliwy i wytwarza odgłosy eksplozji w głośniku lub wciąż się domaga większej pojemności procesora, tak, że normalna praca komputera zostanie sparaliżowana.

WARIANTY: HM2: Wirus nie powiela się. Wykonanie zarażonego pliku powoduje zawieszenie się systemu.

Plastique4.21: Wyróżnia się tylko możliwością samodzielnego kodowania.

Plastique COBOL: Zawiera słowo ´COBOL´; pliki COM rozrastają się o 3004B; pliki EXE o 3004-3019B; wirus staje się złośliwy, jeżeli data systemu leży między 1.01 a 21.09; system zmniejsza swoją prędkość obliczeniową i po 20 minutach, możliwości systemu wynoszą 50%, a po 30 minutach klawiatura staje się nieczynna i pamięć konfiguracji systemu CMOS zostaje na nowo przez wirus zapisana. Od 22.09 rozpoczyna się stan spokoju i trwa do stycznia następnego roku.

PLASTIQUE-B

ALIAS: Plastic Bomb, Plastique 5.21, Plastique 2, Anticad
WIELKOŚĆ: 4096
TYP: rezyduje w pamięci
wirus łączący się
atakuje sektory startowe dyskietek
atakuje pliki COM i EXE
nie atakuje COMMAND.COM

OBJAWY: Ulepszona wersja wirusa **PLASTIQUE**; działa zależnie od daty systemu; zarażone pliki COM i EXE rozrastają się o dalsze 4096B.

DZIAŁANIE: Przy pierwszym starcie zarażonego programu instaluje się **PLASTIQUE-B** rezydentnie w pamięci. Wirus zajmuje 5120B i zapisuje się:
- w dolnym obszarze pamięci, jeśli data systemu leży przed dniem 20.09 danego roku;
- w górnym obszarze pamięci, jeśli data systemu leży po dniu 20.09 danego roku.

Każdy otwarty lub zastartowany plik COM/EXE zostanie zainfekowany.

Wirus **PLASTIQUE-B** sektor ładowania włożonej dyskietki do stacji dysków. Jeżeli data systemu znajduje się po 20.09.1990 roku, wirus będzie złośliwy i wytwarza odgłosy eksplozji w głośniku komputera lub wciąż się domaga większej pojemności procesora, tak, że normalna praca komputera zostanie sparaliżowana. Poza tym, po przekroczeniu jakiejś ustalonej wartości licznika zainstalowanego w wirusie, do wszystkich stacji dysków zostaną wysłane bezsensowne dane.

Slayer Familie

ALIAS: Brain Slayer, Slayer
WIELKOŚĆ: 5120
TYP: zaraża pliki COM i EXE

OBJAWY: Zawartość plików COM i EXE ulegnie zwiększeniu; występują zmiany w katalogach; nieoczekiwany dostęp do wszystkich stacji dysków; nieoczekiwanie długie czasy dostępu do dysku twardego.

DZIAŁANIE: Gdy został zastartowany program zainfekowany wirusem, to będą zaatakowane przez **SLAYER** wszystkie pliki COM i EXE w aktualnym katalogu. W zależności od wariantu wirusa, zostaną zaatakowane też programy na innych stacjach dysków. Zarażone programy rozrastają się o dalsze 5120-5135B; wirus znajduje się zawsze na końcu programu. W zarażonych katalogach data i czas nie ulega zmianie. Jednakże może się zdarzyć, że w zarażonych katalogach, na samym początku występują tylko pliki COM.

Co najmniej jeden wariant z rodziny wirusa **SLAYER**, wprowadza ze sobą wirusa **YANKEE-DOODLE**, który po jakimś czasie rozprzestrzenia się w systemie.

WARIANTY: **SLAYER-A:** Zaraża dodatkowo pliki w aktywnym katalogu aktywnej stacji dysku (do dziewięciu plików w podkatalogu), ale nie w głównym katalogu stacji dysku C:.

SLAYER-B: Działa podobnie jak **SLAYER-A**, jednak zaatakowane będą również pliki w głównym katalogu w C:.

SLAYER-C: Działa podobnie jak **SLAYER-A**, jednak zaatakowane będą wszystkie pliki programowe w C:. Poza tym wirus ten zawiera następujące znaki:

´KEYB*.COM KEYB*.EXE BASRUN BRUN COBRUN NETDOS*.COM´
´IBMBIO.COM´, ´IBMDOS.COM COMMAND.COM *.* .. \ .. *.EXE´
´Access denied´

SLAYER-D: Działa podobnie jak **SLAYER-C**, jednak żadne pliki w C: nie będą zarażone, chyba że, z twardego dysku startowany będzie zarażony program.

SLAYER-E: Znany jako **YANKEE-DOODLE-DROPPER**. Przy startowaniu zarażonego programu, zostaną wszystkie programy zarażone w aktualnym katalogu aktualnej stacji dysku oraz niektóre pliki w C:. Po upływie jakiegoś czasu, wirus ten wstawia wirusa **YANKEE-DOODLE** i uaktywnia go. Gdy zostanie wirus **YANKEE-DOODLE** usunięty, to wirus **SLAYER-E** powoduje nowe infekcje poprzez wprowadzanie wirusa **YANKEE-DOODLE**.

Stoned

ALIAS: Donald Duck, Hawaii, Marijuana, New Zealand
Rostov, San Diego, Sex Revolution, Smithsonian
Stoned II
WIELKOŚĆ: [-]
TYP: rezyduje w pamięci
atakuje sektory startowe dyskietek
atakuje tabelę partycji twardego dysku

OBJAWY: Komunikaty na ekranie; zawieszają się RRL-kontrolery.

DZIAŁANIE: Pierwotna wersja infekowała tylko dyskietki 360KB, bez wyrządzania większych szkód, tego wariantu już jednak nie ma. Wszystkie teraźniejsze warianty tego wirusa zarażają tabelę partycji twardego dysku, gdzie główny katalog i FAT będą uszkodzone. Te wirusy rozróżniane są pod względem komunikatów wysyłanych na ekran w czasie startowania systemu.

Startowanie systemu z zarażonej dyskietki przez wirus **STONED**, powoduje, że wirus instaluje się rezydentnie w głównym obszarze pamięci i zajmuje przy tym ok. 2KB pamięci. Odpowiednio wygląda wynik zgłoszony przez rozkaz CHKDSK.COM. Gdy tabele partycji twardego dysku do tej pory nie były zarażone przez wirus, to teraz to nastąpi.

Podczas ładowania będą wysyłane na ekran przypadkowo wybrane komunikaty, najczęściej tego typu:

'Your Computer is now stoned.´

Z pamięci operacyjnej wirus **STONED** zaraża wszystkie dyskietki, które były używane. Przy tym przepisany zostaje oryginalny sektor startowy do 11 sektora, podczas gdy wirus kopiuje się do właściwego sektora startowego. Sektor 11 jest częścią główną katalogu; jeśli był on przed zainfekowaniem używany, to zawarte tam pliki ulegną zniszczeniu. Dla niektórych wersji DOS'a, sektor 11 należy do FAT'u, tak więc przez tą infekcję FAT (tablica rozmieszczenia plików) będzie zniszczona.

Przy zarażeniu twardego dysku, zostaną oryginalne tabele partycji skopiowane do sektora 7, na stronę 0, do cylindra 0, podczas, gdy wirus wpisuje się w miejsce właściwego sektora tabeli partycji. Gdy twardy dysk został przy pomocy odpowiedniego oprogramowania sformatowany, oraz bezpośrednio za sektorem tabeli partycji znajduje się sektor startowy i FAT lub główny katalog, to w konsekwencji zarażenia twardego dysku, może on zostać uszkodzony.

WARIANTY: **PS-STONED:** Bazuje na wirusie **STONED**, został jednak tak zmieniony, że jego odkrycie może być uniemożliwione. Przy ładowaniu systemu nie wysyła żadnych komunikatów na ekran. Poza tym atakuje wszystkie typy dyskietek.

ROSTOV: Podobny do **STONED-B**; nie pokazuje żadnych informacji; zawiera następujący tekst: ´Replace and strike´sowie ´Non-system disk´.

SEX REVOLUTION V1.1: Taki jak **STONED-B**; wysyła na ekran następujący tekst:

´EXPORT OF SEX REVOLUTION ver 1.1.´

SEX REVOLUTION V2.0: Taki jak **Sex Revolution v1.1**; wysyła na ekran następujący tekst:

´EXPORT OF SEX REVOLUTION ver 2.0.´

STONED-A: Taki jak oryginał, nie atakuje jednak dysków twardych. Jest to prawersja. Zawiera tekst: Ýour computer is now stoned. Legalize Marijuana´. Ukazana będzie tylko wiadomość do ´... stoned´.

STONED-B: Taki jak oryginał. Zawiesza pracę systemów wyposarzonych w sterowniki dysków twardych typu RLL.

STONED-C: Taki jak oryginał. Nie wysyła jednak na ekran tekstu.

STONED-D: Taki jak oryginał; atakuje dyskietki w formacie 3.5 i dyski twarde.

STOND-E: Podobny do Stoned-B; wysyła na ekran tekst: ´LEGALIZE MARIJUANA´ poprzedzony sygnałem dźwiękowym. Znajduje się w sektorze startowym i tabeli partycji.

STONED-F: Podobny do Stoned-E; wysyłany na ekran tekst brzmi: ´Twoj PC jest teraz be!´. ´LEGALIZE MARIJUANA´ znajduje się w sektorze startowym i tabeli partycji.

STONED II: Podobny do Stoned-B; jednak wyposarzony jest w mechanizm chroniący go przed odkryciem; Wysyłany na ekran tekst brzmi: ´Your PC is now Stoned! Version 2´, lub także: ´Donald Duck is a lie!´.

Syslock

ALIAS: 3551, 3555
WIELKOŚĆ: 3551
TYP: ukryty (zakodowany)
atakuje pliki COM i EXE

OBJAWY: Pliki COM i EXE będą zwiększone; pliki zostaną zmienione.

DZIAŁANIE: **SYSLOCK** przeszukuje aktywne drzewo katalogów twardego dysku, wyszukuje pliki COM i EXE, wybiera przypadkowo jeden z nich i zaraża go. Plik będzie zwiększony o ok. 3551B (lub trochę więcej).

Pliki będą zmienione. Wirus szuka w zarażonych plikach słowa ´Microsoft´ (niezależnie, czy dużymi, czy małymi literami pisane) i zastępuje je słowem ´MACROSOFT´.

Gdy w środowisku DOS'a (DOS-Environment) wirus znajdzie tekst: ´SYSLOCK=@´, to nie wykazuje żadnej aktywności i od razu startuje program zarządzający systemem.

WARIANTY: **ADVENT:** Normalnie nie powielający się wirus. Prawdopodobnie zwielokrotnianie się wirusa występuje wtedy, gdy został zarażony plik EXE; jego potomkowie atakują tylko pliki COM.

MACHO-A: Zachowuje się tak jak **SYSLOCK**, lecz słowo ´Microsoft´ zostaje tu zastąpione przez ´Macrosoft´.

Telecom

ALIAS: Telefonica, Telecom File, Spanish Telecom-2
WIELKOŚĆ: 3700
TYP: rezyduje w pamięci
ukryty
atakuje pliki COM

OBJAWY: Pliki COM będą zwiększone; całkowita i dostępna pamięć zmniejszy się; twardy dysk zostanie sformatowany; rozsiewa wirus **ANTI-TEL**.

DZIAŁANIE: Jeżeli zostanie załadowany system z zainfekowanej dyskietki, to **TELECOM** instaluje się rezydentnie pod koniec górnego obszaru pamięci, ale zawsze poniżej granicy 640KB; program DOS'a CHKDSK.COM pokazuje o 3984B mniej pamięci. Przerwanie nr 21 zostaje odwrócone. Rezydujący w pamięci wirus **ANTI-TEL** atakuje twarde dyski i dyskietki, które były używane.

W plikach COM, rezydujących w pamięci, przekraczających wielkość 1KB, zainfekowanych wirusem w czasie wykonywania się, następuje wzrost ich wielkości o 3700B; to zwiększenie się pliku nie jest widoczne w katalogu, ponieważ wirus to uniemożliwia.
Data zarażonego katalogu będzie o 100 lat przesunięta do przodu, jednak jest to niewidoczne w katalogu, ponieważ są wyświetlane tylko dwie ostatnie cyfry roku. Na podstawie daty pliku, wirus rozpoznaje, czy dany plik jest już zarażony, czy też nie.

Rezydujący w pamięci **TELECOM** zaraża tabelę partycji twardego dysku, jeśli tylko jego dowolny plik był używany.
Zarażona część pliku przez **TELECOM** nie uaktywnia się, ale po 400 procesach startowania systemu, przepisuje wirus **ANTI-TEL** na pierwsze dwa twarde dyski.

Tequila

ALIAS: Stealth
WIELKOŚĆ: 2468
TYP: atakuje tabelę partycji twardego dysku
atakuje pliki EXE

OBJAWY: Całkowity i będący do dyspozycji obszar pamięci zostanie zredukowany o 3072B.

DZIAŁANIE: Wirus sprawdza przy pierwszym starcie zarażonego programu, czy tabele partycji twardego dysku są już zarażone, jeżeli nie, to wpisuje swoją niezakodowaną kopię do ostatnich sześciu sektorów twardego dysku i zmienia tabelę partycji w taki sposób, że służą one do dalszego zarażania. Do tego czasu wirus nie instaluje się rezydentnie w pamięci i nie zaraża dalszych plików.

Dopiero, gdy system będzie pierwszy raz startowany z zarażonego twardego dysku, wirus instaluje się rezydentnie w pamięci. Całkowita i dostępna pamięć zredukuje się o 3KB, które wirus zajmuje dla siebie w górnym obszarze pamięci, ale zawsze poniżej granicy 640KB. Wirus zabezpiecza się przed nowym zapisem przez inne programy.
Gdy wirus rezyduje w pamięci, zaraża każdy wywołany program EXE. Wirus dopisuje się do końca programu i zwiększa go o 2468B, jednak to zwiększenie się programu, nie jest widoczne w katalogu, ponieważ wirus rezyduje w pamięci.

Następujący niezakodowany tekst znajduje się w ostatnim sektorze zarażonego twardego dysku:

´Welcome to T.TEQUILA´s latest production.
Contact T.TEQUILA /P.O.Box 543/6312 St´hausen Switzerland.
Loving thought to L.I.N.D.A.
BEER and TEQUILA forever !´

Porażone wirusem programy zawierają tekst w zakodowanej formie.

Zaatakowane systemy, przy wywołaniu programu DOS'a CHKDSK.COM zgłaszają komunikat 'Błąd przyporządkowania plików', gdy wirus rezyduje w pamięci. Jeśli ten program będzie wywołany z opcją /f, to programy mogą zostać zniszczone.

Dokładnie, cztery miesiące po zarażeniu tabeli partycji, w danym dniu miesiąca, wirus staje się znowu aktywny, podając komunikat na ekran:

´Execute: mov ax, FE03 / int 21. Key to go on´.

Przy wywołaniu programu, który zawiera maszynowe rozkazy, zostanie pokazany komunikat z ostatniego sektora twardego dysku.

TEQUILA wirus jest bardzo rozpowszechniony w Europie. Wirus ten został rozpowszechniony przez pewne szwajcarskie przedsiębiorstwo wysyłkowe. Autorzy pomysłu zostali aresztowani. Wirus potrafi się całkowicie zakodować i to w wielu dowolnych wariantach. Jest trudny do zidentyfikowania. Poprzez niektóre zręczne mechanizmy, jest on niewidoczny dla użytkownika i uważany za jeden z najbardziej inteligentnych wśród wirusów.

USSR 1689

ALIAS: SVC V4.00, Off Stealth
WIELKOŚĆ: 1689
TYP: rezyduje w pamięci
atakuje pliki COM i EXE

OBJAWY: Zwiększa pliki COM i EXE; system zawiesza się.

DZIAŁANIE: USSR 1689 instaluje się przez uruchomienie pierwszego zarażonego programu rezydującego w pamięci, w rezydentnej części interpretera rozkazów. Najbliższy program COM lub EXE zostanie zaatakowany, który z kolei będzie przyczyną powiększania się systemu. Zarażone programy zwiększają się o 1689B, ale ten wzrost programów, które przed zarażeniem są większe niż 1689B jest przez wirus skutecznie ukryty. Pliki, które były mniejsze niż 1689B (przed zarażeniem wirusem), będą zwiększone i będzie to zauważalne w katalogu. Wirus dopisuje się zawsze na koniec programu.

Przy każdym zarażeniu programu występuje zawieszenie się systemu i dlatego wirus ten tak szybko się nie rozprzestrzenia, jak inne wirusy i przez to można go szybciej zauważyć.

Vacsina

ALIAS: [-]
WIELKOŚĆ: 1206
TYP: rezyduje w pamięci
atakuje pliki COM, EXE, SYS, BIN

OBJAWY: Pliki COM, EXE, SYS i BIN rozrastają się; sygnał pisku w głośniku komputera.

DZIAŁANIE: **VACSINA** atakuje pliki COM, EXE, SYS i BIN. Pliki EXE zostaną zamienione na pliki COM (pierwsze 2 bajty 'ZM' lub 'MZ' pliku będą w rozkazie JMP zamienione w dołączonym kodzie wirusa, który zawiera własną procedurę przesunięć).

Ten wirus występuje w bogatej formie wariantów (co najmniej 48). Cechą charakterystyczną zarażonego programu jest to, że przy wywołaniu zainfekowanego programu, słychać piski w głośniku komputera; poza tym ulega zmianie czas i data w katalogu, które to (czas i data) zmieniają się na takie, jakie były w katalogu w momencie zaatakowania przez wirus.

WARIANTY: **TP04VIR:** Zaraża pliki EXE i zamienia je wewnętrznie na pliki COM. Zaatakowane programy zawierają tekst 'VACSINA', a przedostatni bajt zawiera binarną czwórkę.

TP05VIR: Podobny do **TP04VIR**, jednakże drugi od końca bajt zawiera binarną piątkę. Poza tym czasami system zawiesza się.

TP06VIR: Podobny do **TP05VIR**, jednakże drugi od końca bajt zawiera binarną szóstkę.

TP16VIR: Podobny do **TP06VIR**, jednakże drugi od końca bajt zawiera binarną szesnastkę.

TP23VIR: Podobny do **TP16VIR**, jednakże drugi od końca bajt zawiera binarne 23. Tekst 'VACSINA' nie występuje.

TP24VIR: Podobny do **TP16VIR**, jednakże drugi od końca bajt zawiera binarne 24.

TP25VIR: Podobny do **TP16VIR**, jednakże drugi od końca bajt zawiera binarne 25.

Vienna

ALIAS: Austrian, Unesco, DOS-62, 648, DOS-68, 1-in-8
WIELKOŚĆ: 648
TYP: atakuje pliki COM

OBJAWY: Pliki COM rozrastają się; system zawiesza się w czasie jego ładowania.

DZIAŁANIE: Wykonując program zarażony przez **VIENNA**, zaraża się następny program niezainfekowany do tej pory (przez ten wirus) w aktualnym katalogu. Plik zwiększa się o 648B, a wirus znajduje się na końcu pliku. W katalogu, zostaną wartości sekund ustawione na 62 dla zarażonego programu. Na 6 zaatakowanych programów, tylko jeden program będzie bez wirusa, ale za to pierwszych 5 bajtów programu zamienione zostanie na skok do procedury uruchamiającej restart systemu. Po uruchomieniu program / system samoistnie ładuje się od nowa. Ponieważ wirus nie dopisuje się do programu, jest trudny do odkrycia przez programy szukające wirusy. Nawet po usunięciu wirusa, mogą powstać nie przewidziane skutki, aż wszystkie zmienione programy zostaną wymienione na niezarażone kopie, co daje gwarancję, że system nie jest zarażony.

Przy niektórych zaatakowanych programach, może wystąpić też zawieszenie się systemu, gdy programy te będą startowane.

VIENNA wirus został zaprogramowany przez pewnego studenta, a program źródłowy tego wirusa został opublikowany, dlatego jest tak dużo odmian i wariantów tego wirusa, i dlatego też mogą wystąpić jeszcze inne symptomy tego wirusa, niż te które zostały wymienione.

WARIANTY: VIENNA 822: Podobny do oryginału, jednak ma wielkość 822B. Nie kasuje plików, nie wywołuje nieoczekiwanego ładowania się systemu (tzw. gorącego startu).

VIEN6: Podobny do oryginału; ma taką samą wielkość; nie wywołuje ładowania się systemu (tzw. gorącego startu). Po zarażeniu 7 plików w aktualnym katalogu, zostaną zarażone pliki w C:.

VIENNA-B: Podobny do oryginału, jednak zamiast modyfikacji restartu jednego z sześciu zarażonych plików, zostanie skasowany wywołany aktualnie program.

VIENNA-B 645: Podobny do oryginału, lecz bez modyfikacji restartu i bez kasowania zarażonych plików.

WIEN: Tak, jak oryginał, jednak posiada środki uniemożliwiające jego odkrycie.

W13

ALIAS: Toothless Virus, W13-A
WIELKOŚĆ: 534
TYP: atakuje pliki COM

OBJAWY: Pliki COM będą powiększone.

DZIAŁANIE: W13 poza czystym zainfekowaniem, nie wyrządza żadnych innych szkód. Jest on spokrewniony z wirusem **VIENNA**, nie uszkadza plików i nie wykazuje żadnych innych efektów, jak wirus **VIENNA**. Poza tym, zawiera on w sobie parę błędów, które mu przeszkadzają w rozprzestrzenianiu się.

WARIANTY: W13-A: Niektóre błędy, które uniemożliwiały rozrastanie się wirusa, zostały usunięte. Ten wariant wirusa ma wielkość 507B.

Yankee Doodle

ALIAS: TP44VIR, Five O´Clock Virus, Yankee Family
WIELKOŚĆ: 2885 oder 2899
TYP: rezyduje w pamięci
atakuje pliki COM i EXE

OBJAWY: Pliki COM i EXE rozrastają się; o godzinie 5:00 (wg. zegara systemowego), zabrzmi melodia z głośnika komputera.

DZIAŁANIE: Jeśli zostanie wykonany zarażony program, instaluje się **YANKEE DOODLE** rezydentnie w pamięci i zaraża pliki COM i EXE. Gdy zegar systemowy osiągnie godzinę 5:00 po południu, to z głośnika komputera rozbrzmiewa melodia Yankee-Doodle. Poza zainfekowaniu plików, nie wyrządza żadnych innych szkód.

Wirus Yankee Family obejmuje ok. 80 różnych wirusów.

WARIANTY: **TP33VIR:** Ten wariant zmienia po kryjomu przerwanie nr 1 i 3 tak, że nie można więcej użyć program Debugger do śledzenia wirusa. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 33 dziesiętnie).

TP34VIR: Podobny do **TP33VIR**, jednak rezyduje w pamięci i zaraża programy, gdy są one wykonywane. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 34 dziesiętnie).

TP38VIR: Podobny do **TP34VIR**, lecz różnie traktuje pliki COM i EXE. Poza tym, wirus sam się odkaża, jeśli program przez CodeView-Debugger wystartowany został. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 38 dziesiętnie).

TP41VIR: Podobny do **TP38VIR**. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 41 dziesiętnie).

TP42VIR: Ten wariant sprawdza, czy system jest zarażony wirusem **PING PONG** i modyfikuje go, w tym sensie, że ten wirus sam się niszczy. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 42 dziesiętnie).

TP44VIR: Podobny do **TP42VIR**. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 44 dziesiętnie).

TP45VIR: Podobny do **TP44VIR**. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 45 dziesiętnie).

TP46VIR: Ta wersja sprawdza, czy system został zaatakowany przez wirusa **CASCADA (1701)** i niszczy go. Ostatnie 2 bajty wirusa zawierają nr wersji (tu: 46 dziesiętnie).

4096

ALIAS: Centurty, Frodo, 100 Years
WIELKOŚĆ: 4096
TYP: rezyduje w pamięci
atakuje pliki COM, EXE, OVL
błędny FAT

OBJAWY: Pliki COM i EXE będą powiększone; system zawiesza się; silne zmniejszenie prędkości roboczej systemu.

DZIAŁANIE: Gdy wirus znajduje się w pamięci, nie wyświetlają się przy pomocy rozkazu DIR zmienione wielkości plików. Wirus atakuje każdy wykonywany (uruchamiany) plik. Niszczy FAT poprzez Crosslinking. Każdego roku w dniu 22.09 system zawiesza się.

OSOBLIWOśCI: Prawdopodobnie, w wirusie znajduje się błąd, który kończy się pętlą programu. Bez tego błędu byłby zmieniany sektor ładowania, co powinno wyświetlić następujący komunikat:
´**FRODO lives**´

DIR-2

ALIAS: Creeping Death (CD), FAT
WIELKOŚĆ: [-]
TYP: inteligentny, rezydujący w pamięci wirus Stealth
wirus sektora startowego
FAT-Crosslinking

OBJAWY: Zgubiony Cluster; przy kopiowaniu pliki zostaną zniszczone; jeśli system będzie startowany z dyskietki, to rozkaz CHKDSK zgłosi zgubione łańcuchy (Crosslinking); CHKDSK /F niszczy pliki !!!.

DZIAŁANIE: Wirus **DIR-2** jest bardzo szybki, uaktywnia się podczas ładowania systemu z zarażonej stacji dysków lub twardego dysku. Jest bardzo trudny do wykrycia, ponieważ nie posiada żadnych widocznych cech charakterystycznych. Wirus nie atakuje plików programowych, lecz zmienia FAT (tablicę przydzieleń plików). Po zarażeniu dyskietki, wpisuje się on do ostatniego clustera na dyskietce.

OSOBLIWOśCI: **DIR-2** wprowadza swój cluster (adres startowy) do FAT dla każdego programu. Oryginalny cluster programów zostanie umieszczony w szczególnym pliku. Jedyny rozpoznawalny efekt to: wszystkie pliki są (crosslinked) w jednym cluster, w którym znajduje się wirus. Próba korekcji tego przy pomocy CHKDSK /f powoduje zniszczenie pliku.

WARIANTY: DC10, DC11, DC12

Parity Boot

ALIAS: [-]
WIELKOŚĆ: [-]
TYP: rezyduje w pamięci
wirus sektora ładowania
Stealth wirus

OBJAWY: Wirus sektora startowego, który rezyduje w pamięci; zgłasza PARITY CHECK ERROR, SYSTEMSTOP.

DZIAŁANIE: **PARITY BOOT** (błąd parzystości przy startowaniu systemu) zalicza się do dość dobrze rozpowszechnionych w ostatnim czasie wirusów sektora startowego. Został on napisany jesienią 1992 roku prawdopodobnie w Niemczech. Od połowy 1993 roku występuje on we wzmocnionej formie. Na podstawie jego szczególnych Stealth-właściwości, znajduje on się w komputerze w stanie utajonym i zaraża każdą dyskietkę sformatowaną na tym komputerze. Wirus **PARITY BOOT** zapamiętuje oryginał sektora ładowania i kieruje każde odpytywanie sektora ładowania do zapamiętanego oryginału, co jest powodem tego, że programy antywirusowe w zarażonym systemie z trudem mogą go zidentyfikować.